Department of Homeland Security
Data Privacy and Integrity Advisory Committee

OFFICIAL MEETING TRANSCRIPT

Wednesday, April 6, 2005
Mayflower Hotel
1127 Connecticut Avenue, N.W.
Washington, DC 20036

AFTERNOON SESSION:

MS. RICHARDS: Good afternoon. Welcome back to the second half of the DHS Privacy Advisory Committee meeting. I move that we open -- reopen the DHS Data Privacy and Integrity Advisory Committee and continue with our planned agenda.

COMMITTEE MEMBER: Second.

COMMITTEE MEMBER: Second.

MS. RICHARDS: So opened.

MS. O'CONNOR KELLY: That's your entire role today is doing the second. Thank you. We pledged when we created this committee that we would hear all voices. I am delighted to have included people that I know and am personally very fond of and cherish their viewpoints. This office and this committee stands on the shoulders of giants and a number of them are kind enough to share their thoughts with this committee's charter about this committee's vision and charter with us today.

We will start with Jim Dempsey, the Executive Director of the Center for Democracy and Technology. Jim, as you all know, has written extensively and testified extensively on privacy and civil liberties, impacts of the war on terrorism. Prior to his service at the CDT, Mr. Dempsey was assistant counsel to the House Judiciary Subcommittee on Civil and Constitutional Rights. He's been a great friend of my office and an open critic of the Department when appropriate. And we thank him for his time today.

I'm going to introduce the entire panel quickly and then we will get started. Parry Aftab, the founder of wiredsafety.org, is an attorney who specializes in internet privacy and security law. Ms. Aftab writes the privacy lawyer column for information in "Week Magazine" and runs an internet safety and help group, Wired Safety, which handles internet privacy, security, and safety issues. She's an outspoken advocate for particularly the safety of our children on-line, an issue that is near and dear to, I should think, all of our hearts. We appreciate her time today.

Professor Peter Swire, Professor of Law, fellow alumnus of an esteemed college in New Jersey that we both went to and a good friend, is the former counselor to the President for privacy under the Clinton administration. He is currently professor of law and the John Glenn scholar of public policy research at the Moritz College of Law of Ohio State University. From 1999 until early 2001, he was the chief counselor for privacy in the Office of Management and Budget. And we thank him for his time today as well. We'll start with Mr. Dempsey.

MR. DEMPSEY: Good afternoon. Thank you for inviting me to speak here today. I have to say at the very outset that I have a doctor's appointment up in Bethesda at three o'clock. And I only got invited to do this yesterday, so I'm going to have to really just blow out of here after I speak. So I apologize for that in advance and that's in no way to be taken as any indication of my respect for this panel or my commitment to working with this panel.

I'm speaking here today on behalf of the Markle Foundation Task Force on National Security in the Information Age. The head of the Markle Foundation and co- chair of the task force, Zoe Baird, very much wanted to be here today but wasn't able to come down from New York.

For the past several years, I've been a member of the steering committee of the task force and Zoe asked me to appear before you on her behalf and to express for her and for the co-chair of the task force, Jim Barksdale, her high appreciation for the work that you're embarking upon and the commission -- the commitment of the Markle Task Force to work with you.

Later on in the second panel, CDT's president, Jerry Berman, who is also a member of the Markle Task Force, will be speaking on behalf of CDT. And so really for both of our organizations, for the Markle Task Force and for CDT, and Jerry will reemphasize this, how much we are committed to working with you as you carry out your work in providing advice to the Department of Homeland Security.

I think that all of you and everybody in this room well appreciates the importance of information and information technology to the war on terrorism. And we also all appreciate the importance of privacy in that process. I prefer to think about those two issues, security and privacy, not as a tradeoff, but as a balance. And I think if there would be a theme for the work of this panel, that would be it.

What is the balance rather than the tradeoff, that we have to have both strong privacy protection in order to achieve the national security goals that we have. And we should not have to give up privacy in order to improve national security. And, in fact, if we were to try to give up privacy, you know, as Benjamin Franklin said, we would end up with neither security nor our liberty. And I think that's because the privacy issues are the issues that help us work through the questions about what information should government be accessing for what purpose, how should it keep it, how should it redisclose it, how do you guarantee or promote the accuracy and timeliness and completeness of that data, and what are the redress mechanisms that individuals should have when they face adverse consequences for the use of that data?

And Zoe Baird asked me to sort of emphasize one message, which is the concern that she has and that I share, that the policy is still lagging behind the technology and the systems development. Time and again, every single report, including the reports of the Markle Task Force, have emphasized the importance of getting the policy right first, that time and again, systems have failed where the policy was not set forth at the outset.

And the American public for all of their concern about privacy and for all of their concern about security and for all of their eagerness to strengthen the national response to terrorism, the American public has shown and members of Congress have shown that they will not accept programs that unnecessarily sacrifice privacy or that do not have sound guidelines and principles.

And the Markle Task Force has stressed throughout the importance of having a privacy framework for information sharing, information collection, analysis, and use. And the legislation, the "Intelligence Reform Act" at Section 1016, which, of course, required the creation of the information sharing environment, specifically as well referenced the importance of having the guidelines and the rules for the collection and use and dissemination of data. And I think that those of you from the private sector, after -- immediately after 9/11 when a lot of government officials and others, commentators, said, well, you know, any direct marketer in the country can get this information or anybody in the private sector can get this information, why can't the government.

And I think what people overlooked in that debate was that the private sector has operated, particularly the credit reporting industry, which had served such an important role as advocators of information, a role in which they're now being somewhat eclipsed by newcomers in the field, but the private sector has operated under privacy rules, the "Fair Credit Reporting Act," for many years and now more recently Graham, Leech, Bliley, and HIPAA. And the principles in those laws, notice, access, collection limitations, disclosure limitations, accuracy and security requirements, redress and enforcement mechanisms, those are exactly the concepts at least that you need to think about in crafting rules for the national security environment.

I think that there's probably not a kind of data or a category of data that should be absolutely off limits to the government. The question is, what is the predicate for getting that information? Is that predicate auditable? Is there a mechanism for sharing that information within a context of rules and guidelines? And that's a challenge that you face, the Department and the government as a whole face, and it's part of an ongoing dialogue that we need to have.

And the Markle Task Force is continuing its work and that work is going on in other forums as well. It will obviously be going on on Capitol Hill as well, but I believe that this committee with the breadth of experience that you have can make a very important contribution to that. And, again, I commit myself personally and on behalf of the Markle Task Force to work with you to do that. Thank you.

MS. O'CONNOR KELLY: Thank you, Jim. Do we have one or two quick questions before Jim must leave the building? Joanne.

MS. MCNABB: Jim, what do you see as the distinction between the Markle Task Force's mission and this committee's?

MR. DEMPSEY: Well, the Markle Task Force, although it has people from, I think, five or six administrations, both the Bush administrations and Clinton and Reagan and Carter administrations are represented on there, people with deep national security experience. It's a volunteer group, which is one of the things that makes it so remarkable. I mean, you are volunteers in a way here, too, but the Markle Task Force has no official status. But I think that at some level, we are all part of an ongoing dialogue. So in a way, I think it's a -- there should be in a way no distinction. We're going towards the same goals.

You have a remit in a way from the Secretary, but the Markle Task Force had a good relationship with Secretary Ridge and we're hoping to have a good relationship with Secretary Chertoff. We've met multiple times with Director Mueller, with DCI Tenet when he was Director of Central Intelligence. We expect to have a good relationship with Ambassador Negroponte. So I think that, you know, as I said, we're engaged in a dialogue and we all have multiple hats that we wear and sort of overlapping responsibilities. In this context, you all are putting aside your private sector or other governmental hats and coming to the table for this dialogue and that's part of this overlapping grouping.

Reverting to my CDT hat, CDT is convening its own. I know individual companies are convening dialogue to try to sort out these issues. And I think it's from that that we're going to get the right answer, but we need to do it quickly because these processes are going forward. Agencies are being stood up and also obviously we face a very genuine threat.

MS. MCNABB: Thank you.

MS. O'CONNOR KELLY: One more question for Jim.

MS. LEMMEY: I just want to follow on to Jim's comments about the separate -- what Markle – the Markle Task Force does versus the committee wearing my Markle hat for a moment. We focused our attention on optimizing information for national security while holding the privacy issue dear. We did not focus primarily on the privacy issue. We looked at the entire system for intel analysis and movement of information from the state and local all the way through to the federal with the element of privacy being driven into it. And I think that the committee here is much more focused on what are the specific privacy rules. So I think that there's a lot of complementary overlap, but they're a different mission.

MS. O'CONNOR KELLY: One more person itching to ask a question.

MR. HARPER: 'Cause I insisted so boldly. I've had concerns about the Markle Task Force report. And, Jim, you might not be the perfect person to ask this question. But with the issuance of each of the two major reports, I've asked Markle staff to tell me who -- what the qualifications were to be a member of the task force and then who was allowed to participate in the task force 'cause I continually came across people who had some role or other in drafting some portion of it, but weren't members, but were somehow associated. Was there any formal process by which people became task force members or were people

excluded? Were people invited? Because, again, I had some trouble with the results of the task force, frankly, and some of the people participating work for companies that have top secret clearance and arguably are part of what privacy advocates would call the surveillance industrial complex.

MR. DEMPSEY: Yeah. As do some members of this committee as well. And I think, you know, we all are involved in this set of issues. I think the Markle Task Force at least sought balance. And people came to the table committed to dialogue. And those who came with a particular point of view, I think, were all committed to listening. And I think people's minds were changed. Okay? And I think this is a crucial point actually, which is so often in Washington, all we do is we go -- and I could give the other -- you know, I could give the other guys comments just as well. And he gives his comments and I give my comments and I never change my mind and he never changes his mind. What we were committed to in the Markle Task Force was changing our minds and trying to find a common ground and to try to understand each other. And we spent the time at it. And that, I think, is reflected in the product of the task force. And I hope it will be reflected in the product of this committee that to put aside the corporate self-interest, to put aside the sort of short-term or the sort of, you know, settled kind of what you've always said and try to find common ground. That's what we did in the Markle Task Force and I really hope and expect that you will do that here as well.

MS. O'CONNOR KELLY: I know you need to leave, Jim.

MR. DEMPSEY: Madam Chair, thank you very much.

MS. O'CONNOR KELLY: So thank you for coming. I appreciate it.

MR. DEMPSEY: Sorry again. A hundred percent committed to working with you. Thanks.

MS. O'CONNOR KELLY: Thank you, Jim. Parry.

MS. AFTAB: Actually, I think Peter is going next.

MS. O'CONNOR KELLY: Okay.

MR. SWIRE: We just thought the subject matter fit slightly better. Well, thank you, Nuala, and to the committee for asking me to be here for today and I, too, would be glad to work with you all in whatever capacity you'd like to talk about these issues. I have a Power Point slide that the committee has copies of and there were copies in back and I think we ran out. Maybe high demand. Who knows? And I'll try to have that up on my web site by tonight or early tomorrow at peterswire.net.

But the talk that I'm giving is the need for government-wide privacy policy. You're a committee of the Department of Homeland Security. I think you'll find that a lot of the issues that are most pressing on privacy are really beyond one agency. And because there is no similar other open committee in the government right now, I think you might have a very important role to play in helping to think about the institution for privacy protection.

So the question is, how do we build privacy in a world of information sharing? And as we try to think about the institutions, I'm going to focus on two topics. One is the "Chief Privacy Officers Bill" that was passed in December this year and the other is the Privacy and Civil Liberties Oversight Board that was included in the "Intelligence Bill" that was also passed in December. So I'll try to link those up to the mission of your committee.

Much of the policy debate on privacy and on substantive rules about privacy, what kind of notice, what kind of access or correction, but as the advisory board, I think you can also play a very good role on thinking about the institution that will over time day in, day out build appropriate privacy into government action. And so you can look to and consider specific recommendations that will lead to better institutional response. Your advice shouldn't just be on the substantive rules.

The first set of institutions to think about is the chief privacy officer function, which Nuala Kelly, of course, is the first statutory position of a chief privacy officer. And I was pleased to get to testify in front of the House Judiciary Committee when that was being considered and delighted that it's been created. And then that, I think, served as a really important model for the bill this past year that required a CPO for every federal agency. And for the agencies that have many privacy issues, and I think you heard this morning that DHS has many privacy issues, having an office day in and day out working on this is a very valuable thing.

Now, Chairman Tom Davis in the House has criticized that law and suggested it ought to be repealed, that we ought to roll back the CPO law, and said beyond that that the CPO function should be subordinated and put within the department of the CIOs and agency, the chief information officers. And his rationale is that will promote unified responsibility and accountability over information system, so let's put privacy where it belongs, under the CIOs.

I'd like to say based on my own experience in government that I don't think that's a good idea. I don't think that's the way CIOs most often think about issues. I don't think it will do a good job for either running the information systems or running privacy policy. And to illustrate this, I'd like to draw on my experience in 1999 when we created a process to set up federal privacy policies for web sites across the agency.

CDT was kind enough to do a study shortly after I went into government that found out that only a third of federal agencies had any privacy policy up. And that was really embarrassing because we were going out making speeches about how important privacy policies were, but we hadn't done it ourselves.

And in the wonderful way of transparent government, they got to do a report and we got to be embarrassed. And out of that came a process where we tried to gather together the people it would take to have good privacy policies for federal agency web sites. One of the people of the seven or eight on the core committee was the CIO for HHS and her role was absolutely wonderful and very helpful. But it's, I think, relevant that it was one out of the seven or eight people -- we had general counsel people, "Privacy Act" people, FOIA people, people with experience with archives, a lot of different functions, almost all of

which were policy functions that had only a limited amount to do with running a technology system. And we rolled it out for -- as an OMB circular and asked for comment on it.

And those policies went into place and have been the foundation of the federal agency policies we have today. They were formalized in the 2002 "E-government Act."

Now, what did we learn from this? One was at least this accidental experience or one experience that CIOs were part of a process but not leading the privacy policy process. But from having worked with the CIO counsel and from having worked in this instance, my own view is that many CIOs do not feel comfortable with a lot of the squishy policy issues. They don't feel expert at making those policy decisions and they look to policy people to figure out when is the right time to have a certain kind of redress, when is the right time to do notice, and the rest. So based on that experience, I think subordinating privacy to CIOs would be a bad move for actually doing the policy well.

Now, there are some flaws in the "Chief Privacy Officer Statute." There was some bad drafting, I think a lot of people have noticed, that puts too big an emphasis on expensive outside audits of agency privacy activities. But I think the other biggest worry about the statute is that it's fundamentally mismatched with information sharing. Right? So many of the issues today are about information sharing often across agencies, across functions.

What have we siloed? We have siloed the privacy function. We have the CPO for Department of Homeland Security. We have it for Justice. We have it for this agency and that agency. When you have multi- agency issues, you should have multi-agency privacy policy. And we've made the old mistake of siloing it. And so as people consider the "CPO Statute," there needs to be a coordinating mechanism, probably in the Executive Office of the President, to do that. It's missing from the statute. It's something you can recommend if you think siloing privacy policy is a bad idea.

Now, there was also in December in the "Intelligence Bill," in the separate bill, one across-agency privacy institution that was created. And I think this is a very good thing. It's called the Privacy and Civil Liberties Oversight Board. It applies to intelligence activities, which is an important component. It's not all the privacy activities of the government clearly, but it's important. The statute says in the Executive Office of the President and it was, I think, fairly understood as a quid pro quo for information sharing in the "Intelligence Bill."

The share network that Markle supported, the intelligence sharing network that's key to the "Intelligence Bill" has the idea that we're going to flow a lot of data between a lot of agencies for intelligence purposes. And Congress wrote into the bill and President Bush signed the bill to have oversight and privacy as a quid pro quo as part of that. The idea is you're going to share the data and we're going to have a process to watch that it's being done in a good way.

As of today, there are no appointees to the board. As of today, there's no staff or other creation of any sort of the board. So I have a simple proposal. Follow the congressional

intent. Follow the quid pro quo. Do not fund any of the share network activities until the oversight board is in place. That's what the statute said. That's why the share network and the oversight board were passed together. So it's simple. It might sound radical, but it's easily solved.

If the administration creates the board, puts the people in place, everything goes forward. But until that deal is done, until you have the oversight, don't make the mistake of building the system with no policy apparatus in place. So to wrap up in the short comments we have, I suggest the Advisory Committee should consider what institutions will improve privacy policy. Agency CPOs are an essential part of the mix, but we should not have siloed privacy policy in an information sharing world. Don't make the mistake that privacy is simply a technical issue for technologists only that should be managed by CIOs.

Do insist that the Privacy and Civil Liberties Board be implemented as a prerequisite to the new information sharing in the intelligence world. And finally, help build agency-wide and government-wide privacy so that we achieve national security but do it with a good policy and the good civil liberties that you all are here to help protect. Thank you.

MS. O'CONNOR KELLY: Thank you, Peter. Questions for Peter?

MR. LEO: Yes, Peter. I'm Joe Leo and I served as the CIO during your tenure. I'd just like to comment and ask a question. The comment is that I think you're essentially on the right track because as the CIO of a major cabinet department, we only had to run to the Office of General Counsel who had purview over all interpretations of the "Privacy Act." And I dare say we used to run over there for "FOIA Act" as well. We could not have legal services attached to our office unless they belonged to the OGC and we paid for it. And the bottom line is thanks to the legal profession, they have missed the -- they have their own code of communication just like the CIOs have in the technology arena. And the complexity of both require some separation as long as the CIOs have a seat at the table.

But my comment goes to one of the problems which is I sat in many a discussion with the Department of Justice over some issues of privacy as well as at the time big discussions on HIPAA. And I thought I was an educated person, but I could not follow all the legal, the journey. And so how, if you have a suggestion, how do you demystify to some degree the legalese of the "Privacy Act" or privacy implementation so technologists have an easier way of putting that into practice or putting that into the systems as they're being built?

MR. SWIRE: Well, first of all, it sounds like on the basic point of whether privacy should be under the CIO that you tend to agree that that would not be the right fit. And then you ask a question about how do we get these different languages and cultures to mix essentially. One of the ways I suggest is you try to have some of the lawyers and policy people who are immersed in technology involved. There are people on both sides of the communities who are bilingual. I think one reason I was hired to my job was I had written my first article on cyberspace and law in 1992 and there was some thought that maybe I could talk technology and talk policy both. And so working with the CIO counsel, I co-chaired a subcommittee with the CIO counsel when I was in government. So I think you look for bilingual people and you look for institutions that are designed to have both

involved. If you screw up on either side, if you have bad policy or bad technology, you fail. And so day in and day out, you have to build sets of people who can talk to each other.

OMB and the information policy and technology grants is one place that that happens. NIST, the GSA government-wide services. There's a variety of places around the government. And I think there's room for greater policy leadership and greater work of these bilingual people than has happened recently. There hasn't even been a White House electronic commerce working group in recent years. I think these are lax and they reduce our ability to respond.

MS. O'CONNOR KELLY: Other questions?

MS. LEMMEY: Peter, I agree and concur with your comments. I think what we've seen -- what I've seen so far is that MOUs are locking people down in ways because they're not really understanding some of the underlying privacy issues. One of the things, though, I want to probe on is you talk about the technology group and you talk about the privacy group having conversations, but that leaves out the people who are trying to get something done. It's people who are trying to --

MR. SWIRE: It's for the mission.

MS. LEMMEY: Yes. And I think it's really critical that the mission really be the focus of what you're trying to deal with. And I just wonder sort of, you know, why -- where do you put that in this discussion?

MR. SWIRE: Well, I think that -- and I think the title of my talk was the need for government-wide privacy policy, some ability to do things across agencies. And a lot of the most important missions are done with more than one federal agency involved. Now, I think the -- what it tends to be -- the way that it tends to work out in practice is clearance. OMB has clearance for congressional testimony, for other initiatives. This is boring government speech, but I think it's -- we're talking institutions here.

And what happens is the mission people come forward with their proposal. They've worked within an agency. They've had a variety of working groups to work it up. And what you hope is that there's been some good technology and policy people involved early. And then what you hope is as the mission is going forward that there's a good review to see if it makes sense for the technology and policy things that people care about. And that's a policy process.

OMB traditionally plays a big role in that. And I'll just repeat again that I don't think we've had as much of that process in the last few years. The institutions haven't been as creative. Nuala has done it for Homeland Security, but I'm not sure who's been able to talk to the mission people and to the technology and the policy people and bring them together sometimes in other places.

MS. O'CONNOR KELLY: Ramon and then Joe.

MR. BARQUIN: I just wanted to bring us back to this second piece of the committee which is integrity because while I understand our real concern with privacy, it just sort of was triggered when Peter suggested no contracts being given on information sharing. But, of course, integrity is central to the quality of anything that we're going to be sharing. And it's very, very much at the heart of some of the things that I believe will be consequences. If there is no data integrity, it's going to have significant consequences on the privacy side on either side. And I just think that at some point, we'd really need to focus on that too.

MR. ALHADEFF: Thank you. Yeah. I mean, I wanted to focus on one thing that Peter raised, which was kind of a sideline, which was kind of the issue of the timing, because internally we learned within the company that privacy needed to be a team sport. You needed to do a consultation and you needed to do it early. And the reason you needed to do it at that point in time was when people make decisions with limited information and no exposure to the other factors that they need to think about, they will unintentionally make the wrong decision, not because they're intending to do the wrong thing, but because it seemed like the expedient and proper way to do it. And it costs a lot more to put the band-aids on it at the end and try to reengineer it than if you got it right the first time. And I guess the question that comes out of the comment is, in your experience when you were doing the privacy coordination, how do you get the consultation to happen early as opposed to in the band- aid stage?

MR. SWIRE: Well, one of the answers is there was that letter B in OMB. That's the budget. You know, agencies want money and so that -- you know, I think that was one of the logical reasons for having a function there, to sort of get their attention as they're planning systems. And one thing that we began and that has continued at OMB is that agencies in their budget submissions to OMB have some privacy-related reporting that's supposed to help drive that into the planning at an early stage. So I think that's one of the ways. I think that happens in companies too. You get their budget. You get their attention. And that's --

Maybe I could think of another point after that, but I think I'll leave that as my main point.

MS. O'CONNOR KELLY: One more question -- two more questions for Peter. Lisa.

MS. SOTTO: Thank you. Peter, are you endorsing sort of an overarching set of privacy principles for the government and, if so, A, what would that look like and, B, wouldn't that be or would it -- I should not state the negative -- would that sort of set of principles be just so watered down because of its broad applicability that it would not necessarily be worth the paper it's written on?

MR. SWIRE: I focused my remarks on what institutions we do rather than a set of substantive rules. Substantive rule sounds a little bit like principles. There's times when you do it. So for our web policies across agencies, we said it should contain at least these things because I think that kind of consistency and having minimum standards made sense there. So there was some pretty clear guidance for a common thing, writing a web page, what you're supposed to do about it. But to imagine that a set of fair information practices would apply to VA hospitals as they're doing medical care and also to intelligence

activities and also to ordinary sort of Fourth Amendment policy searches and the rest, there's just an awful lot of different pieces there. And so I -- we did not spend a lot of our time trying to announce that set of principles. I think that there's -- it's probably outside of this committee -- I've already pushed the committee to think multi agency -- it's probably outside the committee's scope to imagine to what extent the whole European model is better or not. The European approach is to have some overarching principles with a ombud's person at the top and try to have that guide policy. That hasn't been a very good fit with American institutions up till now, I don't think. And so I'm not coming today to suggest that that's the right way to go.

MS. O'CONNOR KELLY: Professor Hoffman.

MR. L. HOFFMAN: Peter, you proposed that no contracts for information sharing systems until the board is in place. Would you consider anything broader or deeper than that? For example, at, I think it's NIH, or maybe it's broader than NIH, there's an ELSI -- at least was an ELSI policy, ethical, legal and social impact statement, where you couldn't get a grant or a contract and certain aspects of things until you had addressed in that proposal privacy or in this case ELSI issues. Would this thing work or not in this case?

MR. SWIRE: Well, it's a topic I believe you and I discussed previously and I think it's a topic that's worth considering, especially for new systems, for new research efforts, and for major new initiatives. Building in ethics, social values, privacy, these sorts of things early is likely to be a big help. If the band-aid comes later, it's more expensive and not likely to stick. And so I think, for instance, for HSRPA, it's well worth considering whether there should be an ELSI percentage. And I think more generally for major new systems, if you were going to pick one of the -- one or two or five of the major systems from today, having ELSI as a component of that is likely to produce better policy results down the line if you build it in from the start.

MS. O'CONNOR KELLY: I'm going to ask that we move to our next speaker since we are now running over. Parry. Thank you.

MS. AFTAB: Thank you very much for inviting me. I'm honored. I made a comment last night to the Secretary that with all of the top privacy people in the country, sitting on this one committee, I'm not sure what anyone else will do. When I turn on privacy issues for wired safety or any of the work we do, I turn to our Advisory Board members and half of them are sitting on the table in front of us. So I should just be doing sort of state of the union on our nonprofit. So you've done a wonderful job.

And before I begin, I think it's very important that we understand a lot of this is about trust. We can talk about protocols and we can talk about check lists, but a lot of it has to do with the trust of the people who have their heart in the right place and then building the framework that will help them comply. And a lot of people I trust extraordinarily at the table in front of me and, Nuala, I put you at the top of that list.

Now, I'm going to be talking about corporate compliance and problems there. I'm going to be talking about kids and I'm going to be talking about consumer understanding of what's

going on. I am not the great thinker on privacy, but I'm a good translator. So you guys come up with great ideas and what needs to happen and I take it and translate it to the simple people who understand the language I speak. People who don't read – "the Economist" read "People Magazine." You know, that's sort of where I go.

Now, I write the privacy lawyer column for "Information Week." And I get to write anything I want and a large part of the time, I spend my time trying to warn corporations how to stay out of trouble. So what's the return on investment to staying out of trouble? It's not huge. It's not the kind of thing the CEO is going to back. It's not a big profit margin.

And most of them don't think about what they need to do to prepare when the real men in black show up at the door. And that's when the head of security, who's usually a former FBI agent, answers the door and said, sure, you can have anything you want without having read or even known about the privacy policies or NDAs or employee handbooks on what they can turn over.

Then you have the lawyers. If they answer the door, they say you can't have anything at all until the Supreme Court rules, after all stays are completed, and all times for appeals have lapsed.

I think that what we need to do is recognize that a lot of this on real security and where we need to go is about preparation. It's about communication. I think that what we need to do is give guidance using the people here on the tables who have done a great deal of this work before and the rest of us to turn around and say you have to think now.

So if this happens, what can you do to prepare? I went to the Homeland Security web site. It's a lovely web site. It's hard to navigate for regular people. And I think that one of the things we need to do is fix that. And Zoe Strickland has a wonderful web site for postal and I think we should talk to her.

But if we can put a guide, some guides on frequently asked questions for corporate compliance officers for corporations what to do when homeland calls and do it up ahead of time. How to prepare in advance, how to check your privacy policies, your human resource manuals, your NDAs, and make sure that they all fit.

You think of the problems on dealing with this government-wide, you can image how hard it is dealing across the corporation people who have no idea what they're collecting and how to use it and when no one is really the gatekeeper. That would be very important. And I think we can advise corporations to set up the one person to answer the phone or the door when you come calling so you make sure you get what you need and you do it in a way that's not going to leave them open to lawsuits later on because they're trying to be helpful. The second thing is communication.

You're having a lot of advocates here and a lot of us wear different hats. The only way you get media and the only way you get funding and the only way you get attention in advocacy arenas is to announce that the sky is falling. Then people would give you money to fix it. If you say the ceiling looks really good, the sky is just perfect, no one is going to

give you a dime or ink. So you're going to get a lot more criticism. I think it's important that we give people credit for those who are doing things right.

A lot of people on the board in front of us, a lot of other people that we know of who are doing it right. They thought about it. Since there's no return on investment for this kind of thing, share. If you've got a check list that works for you, you've got a program that works for you, you thought about the best way to write your compliance policies, share it. It's not the kind of thing that's a profit margin issue and I think we need to encourage more of that, things that are working, giving people credit for what was right.

I was writing an article on the passenger name records and that was when I first saw your writing, Nuala, when you had done the report. And I realized that a lot of the reports that were saying really terrible things, there were a lot of misreports in major newspapers about where the information is going, how much is going, and what happened. I was a lot more concerned about the fact that someone had put a Power Point presentation with someone's Social Security number up on the web without anyone knowing about it. It's the same group that had collected this information then that certain passenger name records were turned over to a government entity.

And I think we need to make sure that real information and balance is given to consumers. We talk about balance. We talk about balancing security and privacy. It's really not about balancing security and privacy. There is no privacy without security, period. And they're interrelated so that when people describe me, I'm described as an internet privacy and security lawyer. You can't be one or the other. You really kind of have to do them both. And I think we need to recognize that when we look at it, they're prongs. They're not balanced. It's not a scale. They're the legs on the table. And we need to make sure that they're all there and we look at it together. So it's more information practices. It's more compliance practices. It's more thinking ahead that we should be dealing with. I also think that talking from the consumer perspective, a lot of people are afraid when they shouldn't be and a lot of people aren't afraid when they should be.

A lot of people think that you have cameras in their bathrooms and in their, you know, hallways and everything else. And they are more concerned than they need to be. We need to let them know that they shouldn't be as afraid as sometimes they're led to be. We also need to let them know when they should be concerned because there are a lot of issues that you deal with that there are gaps. There are information that's being passed around that shouldn't be and there are a lot of those things. We need to let consumers know when to be concerned, when to pay attention, and who to trust. And I think there, the web site could be very helpful as well. I think we need a consumer section, what homeland means to you, what information can be collected from you, what we're doing, what to do if they come calling, what you should be afraid of, what you shouldn't be afraid of, when to call a lawyer, when to open the door. And I think we need to let consumers understand that and there can be some really good awareness messaging that can go out about that. I think there's a great opportunity there.

Lastly children. Aside from the fact that the kids that we work with can take down your website and every other government security website on earth and often do, I think there's

some real opportunities here to recognize both what Homeland Security is doing through your ICE program where they're dealing with sexual predators and sex trafficking or the extraordinary work that Customs and Secret Service has done on protecting people in connection with the internet. You've got fishing and identity theft.

Secret Service is extraordinary there. U.S. Customs has been dealing with child sex trafficking, sex tours to Tsunami regions, and child pornography since long before there was a separate Cyber Smuggling Unit established. And ICE has done incredible cases. I think you deserve a tremendous amount of credit.

And as we look at protecting individuals' privacy, we also need to recognize that there's more here than just terrorism. There's also protecting people's safety and security and that's the balance. So I think we need to look at accountability and give people guides on where to go. Use your web site as a great place to help people understand what homeland security is all about, what it's not about, and that they are in good hands with -- as long as this committee is in place. And the people I know who are there advising it, I'm really happy to be an American and sitting in front of you today. Thank you.

MS. O'CONNOR KELLY: Parry, thank you so much. Any questions for Parry?

MR. MARSH: I thank both of you for your presentations and the comments that you've made in reference to amending the statute, I thought were very, very appropriate. And your comments in reference to the nongovernmental side, I thought were very meaningful. If you look at it, a lot of the problems we have are outside of government. They're occurring in the private sector, both by individuals and by organizations that are using information technology by and large. How do you see reaching these individuals who are engaged in inappropriate collection of information?

And not all data mining is bad, but there are abuses that can occur and there are concerns that are being expressed now by more and more people about the fact that there are encroachments and investigations that are in the private sector that relates to their own lives. Isn't it necessary to create some sort of a culture of ethics that we use? You know, really what we're looking for is as you observed. It's not security versus privacy. We're looking for Aristotle's golden mane. We're looking for that moderation between these two areas. But how do we reach the private sector to enforce this area because government can't do all of it by any means? You can't criminalize it all. How do we reach the nongovernmental sector?

MS. AFTAB: Thank you very much for your comments and I think what you said is very meaningful. I think there's three areas in the private sector that you need to reach, those who want to do it the right way and make mistakes and are sloppy, those who are skirting the edge because there's a line that they think they can cross just a little bit because government can't do everything, and the out and out crooks. I think what we need to do is target the out and out crooks. The guys who are good, they're easy to deal with.

What we need to do is tell them how to do it better so they're not as sloppy and let them know what technology and services are out there, let them know how to comply when they can't afford a heavy-duty CPO, make it easier for them to do that.

"Information Week" that I write for has agreed to help in any way they can on the compliance and getting the word out both for this committee and for Homeland and on any of the things we're doing in private compliance. If we want to try to skirt the edge, we need to let them know that they're going to be caught and if they're not caught by government, there are a lot of advocacy groups and watchdog groups like ours that are looking all the time. Remember what I said. When you say bad things in the media, you get a lot of ink. So what we need to do is make sure that the watchdog groups that are out there looking look a little bit more carefully and have the ear of people who can do something about it in government and make sure that they call the "New York Times" or the "Washington Post" or somebody else when you want to pass the word about people who've gone too far because without trust, we will have no e- commerce. Without trust, we're not going to be able to share information in the best ways. Also our programs with children now deal with good cyber citizenship. It's all about teaching people to control the technology instead of being controlled by it, not to do with what they can get away doing, but doing what's right on-line and off-line.

MS. O'CONNOR KELLY: Thank you so much. Anything else? We are running a little over time. So I'll thank the panelists very much for your time and --- (Applause.)

MS. O'CONNOR KELLY: As we get ready for our next panel, I do want to note again that we are taking comment cards. Both Toby Levin and Tony Kendrick from my office are collecting those and that after this panel, there will be a period of open comments from the public. If you have not signed up, you can do so in the back of the room. And if we have empty time, you can just grab a microphone after the speakers who have already signed up. If you want to connect with the committee or make some comment in writing, you can e-mail Privacy Committee@dhs.gov. That's the Privacy Committee e- mail box. The committee will also have its own web site attached to the DHS Privacy Office web site.

MR. MARSH: Madam Chair, if I might make a comment in reference to our panel, and I know all four of them and they're all very outstanding, but let me mention my former governor. I'm from Virginia. Governor Gilmore performed a national service, not that he's received the recognition he deserves. Several years ago, in fact three years before 9/11, the United States Congress mandated a study commission to look at weapons of mass destruction and the capabilities of the states and municipalities to deal with a weapon of mass destruction and how that should be addressed. They chose a seated governor and I did not see how a seated governor could actually do that, but Governor Gilmore did. He attended every meeting. He was there for all the meetings. He played a key role in developing a report. And out of that, it was very clear that he became a champion of individual liberties.

Many of the recommendations of that report, which took five years to produce -- I served four years on the committee with the governor, so I had an opportunity to observe many of

those -- have been adopted by NIC's Congress. And I would like for the panel to be aware of that particular background which is somewhat unusual. And thank you for your attendance.

MS. O'CONNOR KELLY: Thank you, Mr. Marsh. Indeed, we are pleased to welcome Governor Jim Gilmore, currently of Kelley Drye & Warren, but former governor of the Commonwealth of Virginia, and now partner and head of the Homeland Security practice group at the firm. As Mr. Marsh noted, he was the chair of the Congressional Advisory Panel to assess domestic response capabilities to -- for the terrorism involving weapons of mass destruction or really the Gilmore Commission as we call it. And while serving as governor, he also created the nation's first secretariat of technology, established a statewide technology commission, and signed into law the nation's first comprehensive state internet policy. A

lso joining him on the panel, David Sobel, the General Counsel of the Electronic Privacy Information Center. Mr. Sobel has litigated numerous cases under the "Freedom of Information Act." He's incredibly well-known and well-respected for a lawyer. I think a few of those cases actually may be pending against my Department, I have to say. Seeking disclosure of government documents on privacy policy, including electronic surveillance and encryption controls. He has a long-standing interest in privacy and civil liberties and information policy issues and has written and lectured extensively on these issues since 1981.

Stewart Baker, now of Steptoe & Johnson, with a practice including issues relating to electronic surveillance, national security, data protection, computer security, encryption, privacy, and digital commerce. Currently serves as the general counsel of the Commission on the Intelligence Capabilities of the United States regarding weapons of mass destruction, member of the President's Export Counsel Subcommittee on Export Administration, the Commerce Department's Industry Trade Advisory Committee on Information and Communications Technology Services and Electronic Commerce, and Chair of the American Bar Association Standing Committee on Law and National Security. I think you've done a lot of target practice, Stewart with all those committees, but --

MR. BAKER: That's what my partners think too.

MS. O'CONNOR KELLY: Sorry. Sore spot. And last but certainly not least, Jerry Berman, the President of the Center for Democracy & Technology, founder and President of CDT. The organization plays a leading role in free speech, privacy, internet governance, and architecture issues affecting democracy and civil liberties on the global internet. He's also the President of the Internet Education Foundation, organizes forums for the Congressional Internet Caucus, sponsors conferences on issues such as child safety and privacy on-line, and develops and operates consumer education web sites, such as Get Net Wise. Jerry is an internationally recognized expert on national security and privacy issues. We thank all four of the panelists. I believe we are starting with Governor Gilmore who may have some time constraints today. Thank you, sir.

MR. GILMORE: Thank you, Madam Chairman. First of all, I want to, Nuala, thank you very much for inviting me today. Nuala Kelly and I have testified together up before the Congress several times and I'm aware of how completely dedicated she is to the civil freedoms of the people of this country. So I think you have a good chairwoman. Jack Marsh, thank you for your introduction. Jack served on the Commission for all these years on the advisory panel that was made reference to. No one member of our panel was more important than any other. So I think it's a report that represents a lot of people. I see Paul Rosenzweig, a friend of mine, a colleague at Heritage Foundation when I was working there as a fellow, and then I had a chance to meet all the rest of you or more or less, I think, last night at the reception. I must say I was impressed with how really unruly all of you all really are. (Laughter.)

MR. GILMORE: So I'm happy to be here today. Just a quick summary of the Commission. The Commission was established in 1999 by the Congress by statute. The members of the Department of Defense who were assigned to help set up the Commission came to me and asked me to chair it as a governor, sitting governor. The people who were on it were for the most part police, fire, rescue, emergency services, retired general officers, intelligence people, health care, epidemiologists, people who would actually have to deal with the issues of terrorism and homeland security. Paul Bremmer was on the commission for four years until he went to Iraq. Ray Downey was on the commission. He was one of the chief fire people out of New York City until he was killed at the World Trade Center. So it was a good report. I think it stood the test of time.

In the first year, we assessed the risk and concluded that there was a need for a national strategy. We made that report at the end of 1999. At the end of 2000, we suggested that there needed to be a national office or officer who would be in a position to actually create the national strategy, that it needed to be a federal, state, and local strategy, that there was a certain way that you dealt with challenges in the homeland, particularly relying on state and local people, and we expressed concern about the stovepiping of intelligence.

In the third and what we thought was the final year of the commission, we focused our attention on border control issues, the use of the military in the homeland and how that should be done, how to use states and local people, health care issues, and cyber security. And then the attack occurred. And I was governor of the -- one of the two principal states that were, in fact, attacked that day, New York and the other, of course, was Virginia, because that's where the Pentagon is, in Virginia. So we dealt with those issues that day and including that.

After an extended period of time, the Congress extended the commission for two additional years. In the fourth year, we focused a great deal of attention on the TTIC and the ability to actually create an intelligence fusion center, how counter-terrorism was supposed to be conducted in the United States. Then the last report -- and I've got a copy of that here and these can all be found on the Rand Corporation web page, rand.org. The search vehicle comes up. You put in Gilmore Commission and it comes up.

This was the last report and really the last report after year five. And going out of the door, we expressed several concerns. One that we were losing momentum in terms of homeland

security even as of that time, after -- two years after the 9/11 attack. And second of all, the serious concern that we expressed over the danger to the civil freedoms of the people of the United States based upon the environment in the country after the 9/11 attack. I will say that among the number of recommendations -- and I think that at one point in our commission, we had thought about 140 recommendations and about 130 or so had been adopted in whole or in part by the administrations or by the Congress. The last -- one of the last ones was that we recommended the President establish an independent bipartisan civil liberties oversight board to provide advice on any change of statutory, regulatory, authority for combating terrorism that may have civil liberties implications even from unintended consequences. So we're all happy that you're here.

I think we're a little concerned about the charter, I would think. It's a pretty narrow charter as a matter of fact. I was reading it this morning. It's the first time I'd seen it. It's a pretty close thing. There are a lot of issues, I think, that you may wish to address the issue, but your charter mostly deals with the issue of control of information and how you're going to deal with information. There are serious issues that have to be addressed in the country, whether or not we're going to be really looking at the threat or the vulnerability against this country. The mission, the mission that you all addressed a little while ago, what is the mission that all of us are trying to do? And I want you to be sensitive to the fact that as you go forward, you'll find that there is a tension here that is at work. And the tension is that the mission, there are -- the government is full of people that want to carry out the mission. The managerial instinct to get it done, to deal with the terrorism issue no matter what really, just to protect this country at virtually no matter what the cost is, not allow another 9/11 to occur, which frankly could occur, or to do anything that's necessary managerially to solve this problem.

And, secondly, it is powerfully enabled by the most technological society in the history of the world and that is your writ. How do you deal with this fabulous technology culture that we live in and its capacity to gain information, store information, and disseminate information, and what do you do with it? You see these kinds of philosophical questions shot through so many of the issues that we're talking about today.

For example, the "Patriot Act" is under discussion right now, an issue right now about the issue of real ID cards presently up on the Hill right now. Technologically, we can do astonishing things. One of the previous spokesmen said, well, maybe we should be worrying about cameras all the time, cameras in your bedroom and all that kind of thing. Well, you know, not maybe so much today, but we have the capacity to put cameras anywhere.

Washington, D.C. is quite proud of the fact that you can almost look at any street at any point in time. London is totally proud of the fact you can look at virtually every nook and cranny in London at any time. Not to mention the other technological things like data information gathering, data accumulation, the DARPA program, total information awareness which collapsed precisely because of the concerns and issues that you have to address on this board.

There's a discussion here of balance. I was really fascinated when I came in this morning to listen to the opening because I figure if you see the beginning of a movie, you kind of understand better what it's going to look like as your time comes up. Well, it's interesting that there was this discussion about balance. You know, I just don't think we should be balancing civil freedoms and security at all. I think that you have to maintain the civil freedoms of this country or otherwise the terrorists have won. In fact, they will have achieved something the Russians could never do to us by making us actually transform our culture and our nation altogether. If balance means that there has to be a tradeoff, and there was some discussion at the opening on this, then I think that should be rejected. I think there should not be a tradeoff for freedoms because if you do that, then all the enemy understands at that point is that they have to drive us as hard as they can. And then at that point, we will take more and more spiraling efforts towards ephemeral and shadowy and phantom-like security until all civil freedoms of this country are gone and all privacies are gone. And I'll try to close as quick as I can here because I know we've got four people. But, you know, your writ is about data. It's very interesting.

My sense of things from the charter is that you're supposed to figure out how to control data. You're supposed to figure out how to retain it and the confidentiality of it and how to wall it all off and who's going to get it and who's not and what are the rules going to be and so on like that. And I really wonder if the American people wouldn't say that your writ would be to try to define how much data you're supposed to get in the first place.

The American people, if you really look at it, why are we even talking about privacy? It's only one component of the civil freedoms of the country. And it's because knowledge is power. Knowledge is the capacity to have control over other people. And if the government or private people for that matter have the ability to have knowledge about people in a complete way, then they can intimidate people, freeze and chill people, and change the way people conduct their lives.

So that's a very interesting question about this as to whether it's just as sufficient really for your board to think about how you wall things off. Retention is a very interesting thing. You know, there's a sort of strain that says that some information maybe should be retained and eliminated as soon as possible totally so that the American people can have the confidence of knowing that their information is still private. It has the feel of a technical board, this board, seems to me. But I would urge you to be more of a policy board if you have the freedom to do it and that is to really think about the American character that you represent on this board. The American character which in a large sense has always felt like that if it can just be left alone, it will do just fine. If you can really enable people and empower people, they'll do very well, and they don't want people impinging on them.

And that is what is driving a lot of the discussion and probably why you're here in the first place, to respond to that instinct in the body and the character of the American people, which has always sought to have as much freedom and independence as possible. And now, of course, the question is, what is your role going to be? And I stop by just saying that beginning this morning, Michael Jackson said, you're not window dressing. Well, we'll see. But the interesting question here is what role can you profitably play to enhance the freedoms and liberties of the American people.

MS. O'CONNOR KELLY: Governor, thank you so much for those remarks. I'm sure there must be questions for the governor. (Whereupon, there was no response.)

MR. GILMORE: Well.

MS. O'CONNOR KELLY: They're all cowered by your remarks. (Laughter.)

MS. O'CONNOR KELLY: I think they're afraid. No one? Well, maybe after the panel, we'll have more time to reflect. Oh, we do have one? Oh, we do have one. Thank you.

MR. PURCELL: Governor, I want to just comment. Thank you for those comments. Again and again what we've heard is this balance, tension, dah-dah-dah, all this stuff. I'd like to just echo your comments by talking about the job of the panel is to assure dignity to the individual.

In the early days of technology, Native Americans in North America were worried about photography capturing their spirit. I think what we have to worry about is these advanced technologies actually do capture us. We're ghosted into the machine in very real ways, our pictures, our behaviors, our profile, our histories. We are virtual entities inside the machine. And that -- we need to address the profound obligation that that implies and perhaps even back the truck up a little bit and try and figure out how we can prevent ghosting into the machine in such a thorough way. I agree with you. Americans' security is dependent on our liberty. It's not either/or. It's not a balance. The tension certainly is there, but I'm not secure as an American if other Americans' privacy is not protected.

MR. GILMORE: You know, I think you can do it at the border. After much work in this area, I think you can do a lot of things at the border because there's an understanding if you're going to and from across the border, there's a national, either a foreign country of the United States, but there's some sense that you have to produce a passport, that you have to produce some information and some verification. And that's particularly true of foreigners coming into this country. But inside this country, if you really create a regime that says that you watch and control and understand everything about everybody all the time and use that as a background from which to pick out bad guys, inherently you have to investigate or make every American available to investigation in order to determine he's not one of the bad guys. And that's a challenge because I think it changes the character of the nation. And we have the technical capacity to do it.

MS. O'CONNOR KELLY: John and then Tara.

MR. SABO: Governor, on the issue you raised about knowledge is power, even on the narrow issue of data management, information collection, and so on, what are your views about the degree to which more transparency about the collection of the data, the purchase of the data, the algorithms that are used to process it would help transfer some of the knowledge to the citizens and provide some oversight from either boards or the Congress or advocates? In other words, would not greater transparency about the processes and the data sources and the uses of the data and recourse help even out that power issue that you raise?

MR. GILMORE: Sure. You know, I think that one can come at this from a philosophical and historical perspective and say what government should or should not be doing on an objective basis. On the other hand, you could also look at it from a transparency point of view, just explain to the American people what you're taking and why and under what circumstances and conditions. And then if the American people think that's okay, it will be all right maybe. But if on the other hand, if on the other hand, it gives the American people the freedom to stop improper conduct, like, for example, the Total Information and Awareness Program, that went on the rail strictly because it was not accepted by the public. So, yes, transparency might be a good approach, but just be prepared for the fact that you may get a little rebellion on your hands. But, you know, what Thomas Jefferson said, a little rebellion every now and then is a good thing.

MS. LEMMEY: I'd like to thank you for your comments. And on the recommendations of the civil liberties oversight board that came from the commission, maybe you can share with us some more of your thoughts about what was driving that specifically.

MR. GILMORE: I won't do it long because that's an invitation to talk a long time. But I think the fifth year of the commission, there was a growing sense that we were living in a post 9/11 environment that was pretty hysterical, that began to loosen the bonds of restraint and to provide justification for any type of internal violations of privacy or even potential dangers where without proper transparency and rules and regulations, we were sort of accepting the fact that contrary to the history of *posse comitatus* that maybe the military should be used in the homeland on a regular basis, for example.

The issues of, well, it's okay to ask what your information and data is and put you on record because after all, if we don't do that, then how can we compare you to somebody else that might be a real suspect. The sense that government, even if they have powers that might be used by improper people, ten, fifty, a hundred years in the future, it was okay today because after all, we were only just trying to get the terrorists. So there was a culture and environmental shift that made people very, very nervous. So there was a sense that there should be a board just like this, except that I think you're pretty narrow in your charter, but a board that would really think about these kinds of things and be accountability to the American people for your decisions and bring some sense of light and illumination and focus onto this ongoing debate that should be done and that that would benefit the American people.

MS. O'CONNOR KELLY: We had two more, Ramon Barquin and then Michael Turner.

MR. BARQUIN: I'd just like your thoughts about one issue here, that the ties, your knowledge is power, power to control people, and the issue of the trust that has been spoken about by other panel members too. And one very, very essential component of -- and I'm going to say "government" in quotes because they are the fourth estate that very often wind up to a large degree determining the level of trust on the part of the people vis-a-vis what the government knew and that's the press. Any thoughts for us in terms of how to involve, how to handle, how to work with the fourth estate?

MR. GILMORE: I think there's a constant tension because individual citizens don't always get treated well by the press either. The government certainly is -- the fourth estate is a restraint on government, but it also can be very abusive to people who are entitled to, I think, a certain zone and air of privacy that sometimes they don't seem to get. You know, I think that what you have to focus on here is that tension between the ability to expose information and, thus, root out corruption and badness versus the ability of people to live their own lives, as long as they're not breaking the law.

But with respect to what this panel needs to do, I think that it is to address the issue of whether or not that information can be kept secure and a bond of trust with the people of the United States as information is gained. A lot of the information, I think, is foreign intelligence which may not have a concern.

I think the real issue is what are you gathering on individuals and how are you going to accumulate it and then how will that be used or retained at a later time. I think the people are going to feel a lot better if they know, A, that it's walled off very closely and they know what they've got and what kind of rules are applied to it or, B, that they can't get it at all. And, therefore, people are afraid to go and live their own lives without some anxiety. I hope that's responsive. It's a complicated question.

MS. O'CONNOR KELLY: Just one more question for the governor. We need to get to the other panelists.

MR. TURNER: Governor, I wanted to thank you for your insightful and even somewhat motivational presentation. I just wanted to push you a little bit on your remark regarding the charter and the perceived narrowness of the charter. And I'm not a lawyer and I don't know the procedure for rewriting a charter or whether it can be done. But hypothetically if you could rewrite the charter to broaden it, what would you add?

MR. GILMORE: Well, in two levels. Number one, I think one should be cautious about defining the freedoms of the American people strictly on the basis of privacy. It is true that privacy is essential because then people know that they can live their own lives without scrutiny from their friends, their neighbors, or their government and that is an essential element of liberty, but it's not the only one. There are other fundamental areas as well. But privacy seems to be where the Congress has gone and the government has gone on this.

And then there's the second level and that is the very narrowness of the scope and objectives themselves. If I were a lawyer, I'd be looking for ways to probably give you an opportunity to look a little broader on a more policy-oriented basis as opposed to being technical advisors which I fear that they're asking you based on what kind of computer program is going to work best in order to handle the data in a particular way. And I think, you know, CIOs probably could do that. But CIOs on the other hand are trying to enable, use technology to enable. It seems to me the function of this is to disable, is to try to create some sort of blockage or restraint or oversight or check, if you will, on the ability of technology to impinge upon people. But on the other hand, look at -- if you look at the charter, and I'm sitting here reading it, maybe I'd probably try to drive my truck through B,

ensure the secrecy and confidentiality of information. Confidential from who? Security from who? That's kind of broad. Maybe you all could run with that. Okay? (Laughter.)

MR. GILMORE: Folks, I want to apologize to my colleagues who were kind enough to let me go first, but I have got an out-of-town place I've got to be by six. So with your indulgence, I will depart.

MS. O'CONNOR KELLY: Thank you, Governor.

MR. GILMORE: Thank you.

MS. O'CONNOR KELLY: Our pleasure. Thank you. David.

MR. SOBEL: Thank you. And Nuala was correct about the FOIA litigation. In fact, I believe I filed the first lawsuit ever filed against the Department of Homeland Security. So I particularly appreciate being invited. (Laughter.)

MR. SOBEL: I am also happy to see or was happy to see that this committee was organized under the provisions of the "Federal Advisory Committee Act," which is why this is an open public event and hearing and all within the confines of the Federal Register notice why all of your proceedings will generally be open to the public. But in noting that, I should also say that I was disappointed to see recently that the Transportation Security Administration in creating what it calls the Secure Flight Privacy Working Group, which is a group of outside experts who are reviewing the privacy implications of the Security Flight Program, that group was not created subject to the provisions of FACA and it's also questionable whether TSA has even gone to consider the workings and product of that group to be reachable by the "Freedom of Information Act." So I just want to mention that issue and suggest to this committee that you might want to look at what the Secure Flight Privacy Working Group is doing because, frankly, at least based on some anecdotal information, there's some question as to whether they're doing much at all. But, again, since it's not an open process, none of us on the outside can really look at that.

Now, this leads me into the discussion that I wanted to have with the committee which really has to do with the question of transparency. There's already been some discussion about it. And to take off on the point that the governor raised about what he sees as the limited scope of your charter, I would argue that privacy is actually a fairly broad concept and it's certainly something that I interpret broadly to include issues of transparency and, as I'll discuss in a minute, also due process. So I would urge you within the confines of the charter you've got not to feel too restricted in looking at transparency issues and due process issues.

Now, I think most of the discussion thus far has been relatively big picture. It might seem to you that what I'm going to talk about is little picture, but I think it's really a specific issue which is the Secure Flight Project that helps to flesh out some of the big picture issues that I think you need to look at. And I would also argue, at least from my perspective, that Secure Flight is the most significant project under development right now within the department because it's going to, through its development process, answer a lot

of the questions that are probably going to be raised in the future with respect to other projects. So I'm going to focus on Secure Flight.

I think one of the problems that those of us on the outside who have attempted to monitor the development of first CAPPS II and now Secure Flight have encountered is this transparency problem, specifically TSA's over-reliance on the sensitive security information, SSI, designation. I would refer you to a recent decision of a federal judge in the northern district of California who after conducting an in-camera inspection of information withheld by TSA concerning the operation of the No-Fly list held, and this is a quote, "The government has not come close to meeting its burden and in some instances has made frivolous claims of exemption." So I think this is the one instance we've had thus far where there's been an independent outside judicial examination of some of these SSI claims and that was the court's conclusion.

Now, the effect of the secrecy that has surrounded the program has a couple of effects that I think are obvious. First of all, there can be little public oversight of the development of the Secure Flight Project which is significant given that this is a program that is going to directly affect tens of millions of American citizens in terms of, in effect, having background checks conducted on them by the federal government. I think the secrecy surrounding the project also leads to what thus far appears to be inadequate redress process.

The GAO report that came out last week discussed this issue and noted that the redress system has not yet been finalized and developed, but I think there are some obvious problems that lie ahead for meaningful redress. TSA through all of this has been incredibly resistant to transparency. This probably is best seen in the fact that two "Privacy Act" notices have been issued, one for CAPPS II and one more recently for Secure Flight. The "Privacy Act" generally requires a judicially enforceable right of access to personal information and a right, a judicially enforceable right to correct inaccurate information. TSA exempted first CAPPS II and now more recently Secure Flight from those provisions of the "Privacy Act."

In other words, TSA's position is no judicially enforceable right, citizen right of access or correction. This ultimately is going to lead to serious problems with respect to redress. There are two primary situations that require redress. One, an individual has a name similar to someone on a watch list. He is wrongly matched. Or the situation, a person is the person on the watch list. He maintains that he's been wrongfully included on the watch list. There has to be a meaningful due process mechanism available in both cases.

This is going to be difficult for a number of reasons. First the watch lists themselves are going to be maintained by the FBI at the Terrorist Screening Center. So there's a question as to what recourse either TSA or DHS can really provide when a name is on a watch list. The watch lists presumably are based on classified information, so there's going to be a significant hurdle to due process there. And I think ultimately due process requires some judicial review in its process.

Paul Rosenzweig has thought about this issue a lot, has come up with some very creative ideas about this, and I would commend you to his work and hope that you all can take up this issue in some detail. I think this is important because the Secure Flight methodology is likely to expand to other areas. Already the Transportation Vetting Program within DHS is developing along the same line.

In fact, Secure Flight is now part of that larger program. I think it's also likely that ultimately a system like Secure Flight will be used to vet applicants for employment in critical infrastructure industries. So clearly this is something that millions of citizens rightly have concerns about. What we're talking about here is an unprecedented government role designating citizens as suspect without any explanation for accountability.

The "Privacy Act" sought to establish citizen rights against just that kind of government action. It was created in an era of enemies lists and surveillance of lawful activity. I think just as in the post Watergate period, these issues called out for accountability. The same is certainly true today if not more so. So these are -- this is the issue that I would put before you in my limited time and will be happy to take any questions you might have about that. Thank you.

MS. O'CONNOR KELLY: Thank you.

MR. ROSENZWEIG: One of the things that I'm trying to figure out as we go forward today is the allocation of limited resources, namely our resource. There's a bunch of very smart people here. But so far today, we've been told to -- we've been recommended to look at Choice Point, biometrics, immigration, data security -- I'm leaving out a couple of others. I guess my question to you, David, would be why that one as the priority? What makes that in your mind worth going to the top of the list since we cannot do everything? And I guess as a supplement to that, what would be your kind of second or third choices? You know, how would you order the rest of the priority list since this is your major chance to try and get on -- other issues onto the list? But more importantly, why that one first?

MR. SOBEL: Well, I mean, I think I indicated part of it which is that this is probably the program within the Department of Homeland Security that touches the largest number of citizens. I say tens of millions. But, you know, if you look at it from a perspective of flights and passenger name records that are created, you know, we're talking about hundreds of millions of data records every year that are going to be part of this system. I also think it is a paradigm for a lot of the work that the department is likely to do in other areas in the future and I think it raises some of the most difficult, hard-to-resolve issues that arise in the privacy realm within the responsibilities of the department.

I think the history of this so far has borne that out. You know, this goes back to the days immediately after September 11th when the "Aviation and Transportation Security Act" was enacted creating TSA and giving it, among other responsibilities, the job of conducting prescreening. In the ensuing three years, the privacy problems have proved so far to be insurmountable, so I think history lends itself to the suggestion I'm making which is this is something that really calls out to us to look at.

Among the other issues that you mentioned, I would agree that the Choice Point issue or set of issues is something that is important to look at. I think the important issue there is how government uses private sector information. And I think again Choice Point is kind of a case study of that, but it gets you into sort of the big picture of that whole question of private sector information finding its way into government files and the effect on at least the intent of the "Privacy Act" that that phenomenon had. So if you only had two things to look at in my opinion, those would be two good choices as case studies.

MS. O'CONNOR KELLY: Other comments or questions? Joe.

MR. ALHADEFF: Thanks. David, because you kind of went into some of the mechanics, I guess I wanted to maybe take a step back and ask whether your issue with the program is limited to the mechanics is also associated to the concept or is also associated to the rationale as to why the program is necessary because I guess I -- I want to clarify where your heartburn is coming from.

MR. SOBEL: Well, I mean, I think it's implementation, but only for the reason that, unfortunately from my perspective, the question of concept has already been resolved by Congress. In the "Intelligence Reform Bill," they very clearly spelled out basically what Secure Flight is designed to do. In other words, checking passenger manifests against government watch lists. I don't think that's a good way to spend limited security resources. I mean, I personally, if it was up to me, would spend a lot more time and resources on physical security rather than this idea of focusing on people and conducting in effect background checks. But given that Congress has answered the question in a way that I wouldn't, I am looking at implementation of the system and I think it raises some very difficult due process issues when you're creating a situation where citizens are going to be on some secret government list that they can't see, that they have no right to understand why their name was put on the list and no meaningful way to challenge that. I mean, that is about as tough to ask as you can get and this is something that is in the development process and is likely to be rolled out in a few months. So I think it is a critical issue and, you know, Congress has sort of put us here, but I don't think that ends the inquiry.

MS. O'CONNOR KELLY: Anything else? We do need to move on. And I'd like to encourage the members of the board who have not spoken yet to ask questions of the next two panelists. Stewart.

MR. BAKER: Thanks a lot, Nuala. It's great to be here in front of so many friends. I guess before I start, I think it's only appropriate to say in a gathering like this, there is somebody we still miss. You know, we wouldn't have this meeting without Ron Plesser if he was here and we all miss him still.

I was going to talk about liability and the way in which the case for liability is for security breaches is increasingly likely to be made by an unlikely alliance of national security and privacy advocates. And I'm glad to talk about that. But I thought that since I have emerged blinking into the sunlight from three months of trying to get the WMD Commission's report out that I would give you my thoughts on the ways in which the WMD Commission report might shed some light on the questions that the committee is going to be looking at.

Of course, the commission was set up to look into what happened in Iraq and why we didn't have the intelligence right and to look at some other case studies where we did a little bit better. But it also has a few hundred pages of recommendations for the future.

The good news for DHS is that it only has a few. The bad news is it only has a few because we could never get DHS to return our calls. No. That's not quite true. But the topics that we looked at among other things were information sharing and just a couple of points from that, I think, are relevant also for homeland security activities.

One, we sounded a now very familiar theme which is that maintaining information of this sort, when you're doing that, good national security, good security, and good privacy are not in conflict. They are -- they often need exactly the same kinds of capabilities. That is to say when you gather information about people and you want to make sure that it isn't misused, you need tools to make sure that it isn't misused to take away people's privacy and you need the exact same tools to make sure that it's not misused for intelligence purposes by other governments or other people who have -- who are making an effort to create a national security problem for the United States. So the same kinds of computer security tools that provide for auditing, for determinations as to the reasons for access, the use the information is put to, where it's copied, what happens to it when it leaves a particular database, all of those are tools that privacy and counter-intelligence officials will need and will want. And building the system with those tools in advance is by far the best approach to take. So this is probably the third such observation since Markle made it, but it's nice to see the government sounding moderately consistent on this point.

The second point -- and, again, I don't claim that this is a great insight, but it's nice to hear it said again -- is that the commission recommends that for intelligence purposes information sharing be combined with security so that one official is responsible for both so that the kinds of tradeoffs that have to be made, the kinds of mechanisms that have to be put in place are designed in from the start so that -- and since that in our view security includes privacy, the notion again is that when you're sharing information and designing systems to share information from agency to agency, you should also build in the controls, you should have the person who is responsible for ensuring the privacy involved in the decision about how you're going to do that. That's all, I guess, the good news.

The bad news, I would just suggest that you take a look at our last substantive chapter, Chapter 13, in which we talk about the biological weapons threat and our intelligence capabilities against it. You know, it was really probably 15 years ago that the first computer worm, maybe 17 years ago that the first computer worm. Now we all know you can't spend 30 seconds on there without having downloaded all the proper security tools without being infected, at least if you've got a Windows machine. And that change in climate from unthinkable for computer security worm was released -- to a situation where that's just standard. You have to have protection is a model, at least in my mind, for where we may stand on the -- in the biotech front which increasingly resembles Silicon Valley in 1992. There's a lot of money. Things are getting much cheaper much faster.

And while it's all very wonderful, there's a dark side to this, just as there was a dark side to the internet revolution that we're all living through now. Unfortunately the dark side of

biotech is really much more troubling 'cause you can't, like, just, you know, reboot after Smallpox. The possibility and it is now possible to redesign the 1918 flu which killed -- which would kill probably a hundred million people around the world to release it. And not very many people can do that, but some people can. It won't be long, a few years probably, before it's possible to rebuild the Smallpox virus from scratch or to rebuild it only to make it more fatal. It only kills a third of the people that get it now. It looks as though it's possible from some of the experiments with related diseases that you can kill 90, 95 percent without much difficulty. Those are capabilities that exist now in the hands of maybe, you know, 10,000 people around the world. But that knowledge is on the same downward slope that internet capabilities were on 15 years ago. And we could be in a world very soon where the ability to kill an awful lot of people, even tens of millions, is something that, you know, the smartest guy at Redlake High could do. We have no intelligence capability against that kind of threat. We have no idea how to deal with that kind of threat. And so I do worry that the privacy issues that you're struggling with are going to come back into sharp focus sometime in the next 15 years as we start to see people misusing biological capabilities that now exist just in the hands of a few people. So I'm glad to talk about the liability issue. But I think on that cheerful note, I'll conclude. (Laughter.)

MS. O'CONNOR KELLY: Thank you, Stewart. Questions for Mr. Baker? Yes, David.

MR. D. HOFFMAN: It strikes me that the biological threat is a growing worldwide and international threat not just a U.S. threat. And I wonder if you could talk to the implications of that for this committee and the work that we'll be doing.

MR. BAKER: Yeah. It absolutely is. There's no way in which you can contain either the capability to do this or the consequences of the release of a biological weapon, at least an infectious one so that we can't deal with it simply as a foreign intelligence problem or as a domestic problem. And the solutions to the extent that there are solutions are going to involve from the beginning efforts to establish international understandings or at least to try to extend some sense of responsibility to people doing biological experimentation and working with toxins internationally. And I think there are some recommendations in the report about trying to at least bring foreign companies up to U.S. standards in dealing with toxins today. There's an enormous amount of work that's required there.

MS. O'CONNOR KELLY: Other comments from the panel? (Whereupon, there was no response.)

MS. O'CONNOR KELLY: Thank you so much, Stewart. It is right and appropriate that Jerry Berman gets the last word.

MR. BERMAN: Thank you, Nuala. I don't know whether it's -- it's a daunting task to have the last word. All the distinguished panelists and distinguished Advisory Committee. But I've been trying to listen to everyone and also think back about what we confront as we try to reconcile, balance national security and civil liberties issues post 9/11.

Every time that -- since 9/11, Congress and the executive branch have asked for and expanded investigative information sharing, intelligence gathering, and other authorities to thwart terrorism. And at the same time, there's been a consistent call for protecting privacy at the same time. All the way back to the Department of -- after the "Patriot Act," Department of Homeland Security was established and this Office of Privacy and Civil Liberties Office was set up to coordinate activities to protect civil liberties with respect to information sharing, secure airline flights, biometric IDs. From the beginning, that was the task.

Congress has also said if you don't get privacy right, we're going to put impediments in your way. If you start to go too broad and think of Total Information Awareness, we're going to stop the appropriation for that. If you don't get CAPPS II or Secure Flight screening right, we're going to put riders and stop it. And also if we don't get coordination right, we'll do it again.

So in the "Intelligence Reform Bill," you have a soon-to-be, not-yet-appointed civil liberties board which I think is supposed to perform the same function that the Congress originally thought were to be performed by this committee. In the end, what you have is an expansion of investigative authority, a need for privacy protection and coordination, but we don't know quite where it's vested. The authorities are scattered across a range of agencies. This department, Department of Homeland Security, which you operate, did not end up with the coordination of all intelligence and it's made things very difficult. If you're trying to fix the Secure Flight Program or CAPPS II and you are trying to match ID programs against terrorist watch lists and the terrorist watch lists are controlled not by DHS but by the FBI or TTIC or a new counter-terrorism office, it's very difficult to do that. It's gone outside your jurisdiction.

It's very difficult to deal with information sharing which originally was a concept within the Department of Homeland Security and the original Markle proposal report, which I participated in -- I'm on that task force with Stewart -- recommended that the Department of Homeland Security take charge of reconciling privacy and national security to facilitate information sharing. It has since moved under the "Intelligence Reform Act" somewhere else. So the coordinating function is now under the NID, soon to be appointed, and he still has to sort his thing out and Congress has to -- so you get the point. We have a moving target, a massive set of issues that cross a range of agency lines and involve significant new issues of privacy and national security.

And we don't know who has the authority. I recommend that in terms like that, the way to approach it is to -- I'm going to agree with EPIC -- think smaller. Don't try and perform that coordinating function. I would like to see this Advisory Committee work with the Department and take on the Secure Flight issue. It's the one -- it's the most -- it affects millions of people, but it affects almost every piece of the puzzle that has to be put together. The coordinating function, I've already mentioned.

How do you coordinate terrorist watch lists with ID programs if they're in different parts of the government? This Advisory Committee can speak to that. Can you do this function without new legislation? I'm convinced that you need new legislation because this whole

new era of security risk assessment where the government is using not only government data but also voluntary turnovers from commercial airlines and also purchasing data and working on contractual relations with data brokers bring into issue whether you can have a significant exchange of information between the private and the governmental sector which is outside the system of records of the "Privacy Act" and the "Fair Information" practices which control government systems and records. I think that it is a mistake both from a national security point of view and a civil liberties point of view to go forward purchasing and using information out from under "Fair Information" practices because the same accuracy, completeness standards that you have for "Fair Information" practices are what you want for national security investigations.

And if you don't have them together, you're going to have false positives, Dave Nelsons, Ted Kennedy, and Congress putting strings on a program which is absolutely necessary to replace this crazy thing that happens to all of us at airports. We need a better program, but it can't be implemented without Nuala. It can't be implemented by -- in a privacy no-man's land where the "Privacy Act" is being left behind and a whole range of data is being used. It raises the issue of data mining because you are looking for -- you're using that information for IDs. Do you need a warrant and a judicial process? Do you need a redress process? I mean, what kind of redress process can be constructed by the department?

I think you need Congress to step in and say if people are harmed, this is -- this is an area which Congress is going to come to because if they follow the Choice Point ball, they're going to end up right here, the government use of data, private sector data because it has consequences, serious consequences. And when Congress face issues from "Fair Credit Reporting Act" to financial records where there are potential abuses, where there are consequences, where people can be adversely harmed, that's when Congress passes privacy legislation. And I think it's going to need the recommendations of this committee about does Secure Flight, why isn't it working, what are its impediments, is there a need for more coordination, is there a need for a new statute that governs the government purchase and use, contractual use of data from the private sector, is there a need for a redress system.

Candid advice both to the Department and to the public about whether you think a privacy issue can be resolved without clear law, that's where the Administration has not spoken clearly except in the investigative side, but never on the privacy side. And until the Administration, the Congress, the business community, and the private community figure out that they have to get at the same table to figure that out and you can be a facilitator of that dialogue, in that one case, I don't think we're going to achieve what we want, which is to reconcile these two and important values of national security and civil liberties. Thank you.

MS. O'CONNOR KELLY: Thank you very much. Reed Freeman.

MR. FREEMAN: Mr Berman, thank you very much. That's very inspiring. And I want to echo a comment made previously about Ron Plesser. He was certainly an inspiration for a whole generation of younger but aspirational privacy practitioners. Your recommendation to focus small, I think, is ambitious because it's the rare group that narrowly defines its own mission, but I think it contradicts Professor Swire's think big approach. And I wonder

if there is a way to reconcile that by focusing on a narrow issue, but within the context of that making broader recommendations.

MR. BERMAN: I think I was trying to say that, that if you focus on this case study, it will raise broader issues of whether you need a coordinating function and what, for example, should be the role of the Civil Liberties Board or should Congress revisit that. It will raise issues of whether the "Privacy Act" and currently privacy statutes are adequate to deal with how the government wants to use and compare and do risk assessments.

It will also confront the major unresolved issues of the terrorist watch lists and how are we going to deal with them. And until you can resolve this first screening program, which is critical, all the other screening programs are like waiting in the cue. So I don't know how you can get off this square. This is first base.

MR. FREEMAN: Thank you.

MS. O'CONNOR KELLY: Yes.

MR. LEO: Very quickly, a practical question, timing to tackle that issue. I believe that the GAO looked into Secure Flight and said it isn't ready. Nine out of ten didn't meet Congress' need. And I would like your reaction about whether or not from a timing standpoint the Congress and/or the court step in before this body of brilliant colleagues can really get their arms around the issue, et cetera, et cetera, and step in the middle of what seems to be a front-page, every-day occurrence. So your advice on that.

MR. BERMAN: I understand that it's on the front page, but I'm telling you that if you really go up on the Hill and talk around, no one knows what the answer is. So all the brain power and candle power you can bring on this will be welcome.

The legislative process does not turn very fast. Congress may do something about the identity theft issue that was exposed by the Choice Point security breaches, but it's going to take them a while to sort out. Even though Choice Point has said we need "Fair Information" practices applied to our data, it's going to take a while for that industry to sort out whether they need a statute.

I think that in the security area, that to go forward, it's going to need a -- I think that what we're -- if you permit, we're dealing with credit risk scoring. There's this whole new developing era of security risk scoring in the age of terrorism. And I think that we can't dump it onto the "Fair Credit Reporting Act." I think we need to look at what separate statutory authority, what kind of quality of record, what kind of report, what kind of access, what kind of delayed access to national security, what kind of rules we need to govern this because it's not just airlines. It's baggage handlers. It's employment checks. It's schools. It's going to -- once it's tested, it may determine whether you get into this hotel. And we have to sort that program out before it spreads because it affects national security and it certainly affects many of our civil liberties, not just privacy.

MR. MARSH: Just a quick question. You indicated statutory reform or assistance. Where would you look for committee jurisdiction?

MR. BERMAN: That's another reason why it's going to take a while and you can catch up. (Laughter.)

MR. BERMAN: There is multiple jurisdictions. It's partly under the Commerce Committee and partly under the Judiciary Committee. I wouldn't worry about jurisdictions just like I wouldn't worry about all the bills that are flowing. I would try and say why are we three years later, or is it four years, still stuck? It's not because of David Sobel's litigation, is it? (Laughter.)

MR. BERMAN: He just keeps pointing out that you're stuck.

MR. BAKER: If he's fund raising, then it is. (Laughter.)

MR. BERMAN: Well, if you want to keep supporting EPIC's fund raising efforts, you don't stay stuck. Let me be serious. This is a very serious issue. And you can say, well, let's deal with biometrics and let's deal with, you know, new technologies or let's move on to the information sharing environment. But I think it's going to be 30,000 feet and nowhere. And I think Paul's question about resources, where you put your resources trying to solve a problem that people are wrestling with and can't solve. And if you can solve it, great. If you can't solve it and explain why, it may provide part of a road map about what needs to be done.

MS. O'CONNOR KELLY: We've got one more.

MR. WRIGHT: When Congress established the funding for Secure Flight, they did establish a couple of hurdles, perhaps you might call it road blocks, that the Department had to get past with GAO acknowledgement, that they've gotten past those. In retrospect, do you think that was the right approach, or let me say it a little differently? Do you think Congress asked GAO to look at the right pieces or the right hurdles that were set up before the funding could go through?

MR. BERMAN: Congress is working on the back of an envelope. I mean, it really doesn't know in a fast-moving era what is involved here because it doesn't know what privacy rules to recommend because we don't know what the dimensions of Secure Flight are. It remains to be defined. Is it an ID identification program or is it security risk program? Is it -- what kind of data is it going to use? What are the consequences? So Congress is just doing what it does. It used to in the old days -- I go back to when there was the Office of Technology Assessment -- any time Congress got stuck, it asked the Office of Technology Assessment study it. That meant we need more time. All they're doing here is saying get it right. They don't know quite how to do that. But one of the problems is that if the administration gets it wrong, Congress will say we told you so.

MS. O'CONNOR KELLY: We are now going to move to the period of public comments. I want to thank the panelists for their time this afternoon. (Applause.)

MS. O'CONNOR KELLY: If the folks who've signed up to speak would come to the middle podium.

MS. RICHARDS: So based on the number that you received from Lane or if you didn't, then go ahead and you can start a line back there. And if you would identify your name for the record.

MS. O'CONNOR KELLY: So we're going to try to attempt two-minute comments from as many people as want to comment to the board. And, again, we ask that the speaker identify themselves which is for the public record. Thank you very much.

MR. LEONARD: My name is Steve Leonard. I'm the Chief Operating Officer of an entrepreneurial firm devoted to analytic frameworks to help our customers characterize complex situations. It's been used on the government side in the case of a chemical and biological defense command to characterize tough issues relative to "GPRA," the "Government Performance and Results Act." On the commercial side, it's been used by IBM worldwide to work on new product development. And personally, by the way, like some in this room, I am from the IT space. I spent 17 years at IBM and saw this at work and decided to realize my entrepreneurial urges by joining this entity. Something struck me moments ago as I was looking at my green wrist band, that if I saw one of you at dinner tonight and you saw this still on my wrist, you might say there's a high likelihood, if you don't remember I was standing here, that that gentleman was in the room today. But I can guarantee you that if I walked into my home in Pittsburgh and my 12-year-old son sees this, he's going to claim that I was here at Six Flags today. (Laughter.)

MR. LEONARD: Why am I saying that? The reason I'm saying that is that there's particular context that goes with information. The information being the fact I have a green wrist band. Context relative to that information leads to knowledge and, of course, potentially intelligence if used properly. The work we've been doing relative to putting context on information has in the work we're doing hopefully enabled collaboration, to some degree prioritization, and it's based on, shall we say, holistic dimensions. Well, okay. So we play in this realm of trying to put information into context. We would submit to you that technologies like ours, and there are others, will allow sharing of information at a contextual level to avoid indiscriminate use of the raw data until which time it's justified.

So why am I standing here? As a party who plays in this realm, who has devoted its energies to this topic, we would submit to you all in your thinking that there are solutions, some emerging, some that haven't maybe realized as much attention as others over the years, that indeed can satisfy and contribute to the same tool maybe, both information sharing as well as protecting privacy. That as was discussed earlier today, we would submit to you both can be maximized and there aren't just tools that do one and there aren't just tools that enable the stoppage of information because you can satisfy both.

What I would ask you all for anyone on the commission who's willing to comment is to what degree in light of all that are you going to have a solution mindset? The governor, of course, talked about policy and policy is important and required here. We would look at this -- the composition of this group and say, gosh, there's technology participants here who can contribute to solution thinking and maybe even experimentation to some degree as mentioned. How much does this body intend to look at solutions as opposed to just identifying gaps or policy is my question?

MS. LEMMEY: Well, I can guarantee you I will be since we can't speak for the body because we haven't decided what we're doing yet. But I think that in all the work that I've seen so far in developing solutions around privacy over the last 15 years that in each space, it does require an innovation and a new set of thinking. And I think that this group is very, just by knowing the backgrounds of the people who are here, are very in-line with that thinking. So I think when you come back to our next meeting, you'll probably see some of that.

MR. HARPER: Not intending at all to provide counterweight because I think any solution of any kind is welcome to inform the debate, I have a sense and a suspicion that our focus will be programmatic, that is we'll look at particular things that are being done in DHS. I'm fascinated by what you're describing and have started to study one-way hashes that can reveal context without revealing personal information. But whether that's in any program right now, and we would be considering it, I doubt if we'd be wanting to consider it in the abstract. My gut at this point, so --

MR. ALHADEFF: Yes, just quickly, 'cause I am one of those people who work for also a technology company, but technology, especially as we will consider it, is a means to an end, not an end. So the extent to which it is, in fact, part of a larger way of addressing an issue is the way it's going to be looked at.

MR. BARQUIN: In effect, as we've all discussed back and forth, balance, no balance, balance, no balance, ultimately it is about embedding, converging, a lot of the things that technology and solutions can bring in to the point where a lot of these semantic issues go away, I believe.

MS. O'CONNOR KELLY: Thank you very much.

MR. HILL: Hi. I'm Austin Hill. I'm currently the President and CEO of a company called Synomos, but I believe a number of you know me as the former CTO of a company called Zero Knowledge Systems, which is where we -- I met Nuala when she hired us at Double Click to help them deal with some issues they had. And by CTO, I mean chief talking officer. That's why my voice is rasp. Certainly not technology officer. And so to try and keep to the two minutes, I actually made some notes for myself.

So what I really wanted to talk about was -- and I think we've heard it all day -- the idea of public versus private data have largely started to dissolve in the discussion around national security. And we're really talking about in the information supply chain. And when we start to talk about information supply chains, I'd like to suggest potentially a new charter, although a little bold and arrogant, but those of you who know me are not surprised by that, which is we should be talking about developing an information governance infrastructure.

The concept of information governance, I think, starts to deal with from private citizen to private institution to public institution to the quagmires and the difficulties of managing citizens' right, corporate interests. These are rife with problems. But at the same time, a proper governance infrastructure takes hold of the responsibility of saying how do we

address those problems, how do we begin to manage the process in an area where governance meeting strategic objectives -- that's the definition of governance -- meeting objectives set out by who are you responsible to.

So if we start to think about information governance as our goal, I think we have incredible opportunities to really change how we approach this problem. In the private sector, I did a project with Peter Cullen at the Royal -- when he was at the Royal Bank of Canada and we took a privacy impact assessment process that was currently taking 15 days in their data warehouse group and we changed it to a three-minute process. The project paid for itself within three months. So the efficiencies, the risk management, the benefits that are possible when you start to say what is our objective, it's proper governance. It's improving in the private sector shareholder value. So there's opportunities to begin to do this.

And I guess I would throw out to this committee as a challenge is much like the SEC auditors, corporate boards, chief financial officers, have a well-established infrastructure and Ron notwithstanding for transparency, secure financial markets. There is a process in place. There's always improvement. Sarbanes Oxley was an improvement on that. We have nothing similar to help manage an information market economy and we need to start establishing that. And I think there's an opportunity for this committee to take some leadership in saying how do we establish proper information governance, checks, balances, and goals. Thank you.

MS. O'CONNOR KELLY: Thank you, Austin. Any comments? (Whereupon, there was no response.)

MS. O'CONNOR KELLY: We'll go to our next speaker. Thank you.

MR. VON BREICHENRUCHARDT: Good afternoon. Thank you. I brought my trusty stopwatch with me and if I go over, I promise it will only be a matter of seconds.

My name is Dane Von Breichenruchardt. I'm the President of the U.S. Bill of Rights Foundation. It's a public interest law policy group here in Washington, D.C. And I see one friendly face, Paul Rosenzweig, who I have the greatest respect and I've worked with Paul on a couple of projects. I'm here -- and by the way, I'd like to say, it was a delight to see Governor Gilmore because he speaks like a fellow of Virginia. And I know well. I know now why I voted for him. And I might not be as prickly seemingly after hearing what he had to say, but I'm going to address this from the "Bill of Rights" point of view and I hope you understand that a lot of people I speak for a lot. And I think you'll recognize this.

As we all know -- and I'm not telling you something you don't already know -- going all the way back to the "Declaration of Independence," the federalist papers all the way to the writing of the "Constitution," the Ninth and Tenth Amendment, is that it's always been recognized that the powers that government enjoy come from us. Any autonomy the government gets, they get it from us. And it's an exchange. And to form the more perfect union, of course, we all agree to give up some of the appropriate autonomy to our central government to run the affairs of the nation appropriately. And later came the Ninth and the Tenth Amendment that made it very clear that we did not give up all autonomy, only a

portion of it, and only that which government should have. And we went to the point of saying that they were limited and enumerated.

Unfortunately the federal government, as Paul well knows, has grown from a federal agency of only three laws to now over 4,000 and counting. Every one of those laws to some degree chipped away at our autonomy. Governor Gilmore said that the only issue here is not just privacy. He is right. And it is autonomy. And privacy, I agree, is a currency of autonomy, but we're losing it.

What has happened is every time that there is some sort of foul-up at the federal government level, the answer always seems to be, even when they're told that they're the ones that screwed up, they come back to us, we want more. We want more tools. We want more power. We want more authority. And if you really are honest and look at all of the reports and what has occurred from the 9/11 incident is that the reason that they were successful as they were was not because they didn't have the tools in place to combat it. It happened because they did not have sufficient attention and resources focused in the right direction for job number one, which is to protect the citizens, particularly standing on our own soil. But, yet, they wanted to come back and get more.

One interesting fact is that even in the 9/11 Commission, it was pointed out that one of the great things they got out of Patriot One was the fact that now law enforcement can now share information with intelligence as if we couldn't have done that before. Well, it turns out that one of the commissioners on the 9/11 Commission, she was the one that got it wrong. She misadvised the various departments that they could not share the -- it came out later that actually we could have.

So I guess what I'm asking you to do, and particularly as it applies, like, to the driver's license, you're going to be looking at things like this. And already this is a de facto passport within my own country. If you don't believe me, try to get on any common carrier. Try to check into a hotel. Try to do any significant business without this. And it's already a de facto ID card, a national ID card. And now the federal government wants to slide its tentacles around this.

And I'm always reminded of the arguments on the floor of the House and the Senate when we came up with the Social Security numbering system. There were great fears that this was going to turn into a national ID identifying number. And they all said no, no, no, never happen. Well, today we all know that they might as well tattoo it on our foreheads when we come out of the womb. There is no way you can survive in this country without a Social Security number. And I ask you to consider that maybe some of the advice that you might want to give to this administration, to Congress, and to the federal law enforcement is if you can't get the job done with the tools that we have already given you, maybe you should consider stepping aside because there are other people who say that they can. I thank you.

MS. O'CONNOR KELLY: Thank you for your comments.

MR. HARPER: I'm delighted by the fact that your watch runs a little slow -- (Laughter.)

MR. HARPER: -- because your comments -- because I think your comments are very welcome. This morning I mentioned federalism and separation of power as animating principles that we might consider in our own work here. And I was a little embarrassed by the afternoon that no one had talked about the Fourth Amendment, for example. And I think it will be important, an important part of our work to ground our analysis of different programs in constitutional doctrines and constitutional limitations on governmental power.

MS. O'CONNOR KELLY: Thank you, Jim. Any other comments? Joe.

MR. ALHADEFF: I just wanted to touch on a point that was raised but wasn't amplified and that is the concept of, you know, regardless of whether you like or don't like the fact and nature of the license having become an identifier, one of the most problematic aspects of it having become an identifier is the proof that was necessary to get that document was the proof they thought was appropriate to allow you to drive a car. It was not, in fact, the proof they thought was necessary to allow you to do everything else we want you to do with that. So it was unfortunately a document never designed for its current purpose because it still allows you to drive a car, but it allows you to do a lot more. And so it's not just the issue of whether it's a good or bad thing that it was an identifier, but it's an issue that it doesn't have the proof behind it to be the identifier it currently is.

MS. O'CONNOR KELLY: Thank you. John.

MR. SABO: I think that gets to an issue -- I think it ties in to what Austin talked about and the gentleman's comments and that might be that -- it could be good for the committee to think about -- think a little bit out of the box, so to speak. I don't quite know what that means in this dimension, but the circularity of what you just talked about, Joe, is absolutely correct. When I worked at Social Security, SSA did data matches with the state Motor Vehicle Administrations through Amnivet (phonetic) to establish that an SSN actually was appropriate. And, yet, the -- there's a circularity. The breeder documents could be falsified and then once they're entered into the system, the whole system begins to collapse. So it could be in terms of integrity, in terms of errors, risk management. So it could be approaching some of the issues that the board may approach and stepping back from them and saying are there new ways to approach this that might be perhaps a bit out of the box, but more effective in reaching DHS and getting some play. I think it's something we should think about.

MS. O'CONNOR KELLY: Thank you, John. Any other comments? (Whereupon, there was no response.)

MS. O'CONNOR KELLY: Our next speaker. Thank you.

MS. BENOWITZ: Good afternoon. My name is Brittany Benowitz. I'm with the Center for National Security Studies. First I just wanted to thank the committee for your commitment to having this process partially open and for sharing all this information with the public. I have a question concerning due process. As it cuts across all the agencies within DHS, it's not simply Secure Flight, not simply TSA.

My question is what protections the committee envisions that they could provide against -- for due process as the government has new powers to collect information, to share the information, to help avoid specifically two types of problems. And I'll use the example of something the Under Secretary spoke about this morning regarding that DHS has been concentrating on the use of, for example, HAZMAT licenses and there have already been cases in which people have mysteriously had their HAZMAT licenses revoked and then had them mysteriously restored, presumably because there was some nexus with a security threat. But they were never presented information on what the security threat was. But what we do know, what the public does learn about is that these individuals, for example, share a certain religious background with known terrorists.

And so I think this raises questions about two things. First, what protections will there be against the use of counter-terrorism resources for noncounter-terrorism purposes, for example, using information sharing environment to enforce the immigration laws? And then the related question is, what protections will there be that when there's an adverse consequence related to the collection of information that the nexus with -- of a connection to a terrorist act is very specific and very concrete and isn't left to be so general that it might sweep in many people who share ethnic or religious background with known terrorist suspects, but have not themselves actually had any concrete nexus with terrorism?

MS. O'CONNOR KELLY: Thank you for that very important point. Response, Lisa.

MS. SOTTO: I appreciate that comment. Thank you very much. I think personally, and I'll speak personally, that redress and accountability are critical, the ability to gain appropriate redress. And to that extent, I would hope we would absolutely address due process issues. If we can't narrowly tailor a program such that it gives us exactly the information that we want, then we ought to be rethinking that program. Thank you.

MS. O'CONNOR KELLY: Other comments from the committee? (Whereupon, there was no response.)

MS. O'CONNOR KELLY: Our next speaker. Thank you.

MR. SPARAPANI: Hi. My name is Tim Sparapani. I'm with the American Civil Liberties Union. It's a pleasure to be with you all and I'm glad that you're here and convened. I look forward to working with you and I pledged the ACLU's assistance and sometimes prickly comments when we believe they're necessary. But I do want to thank you all and look forward to working with you. I had remarks prepared and then I found myself in the unusual position of finding an unlikely ally in a room.

When Governor Gilmore gave his comments, I quickly shelved exactly what I was about to say because the governor gave our comments. So if the governor were still here, I would be welcome to invite him. There's still time. You can join us. We've got a card for you to carry. (Laughter.)

MR. SPAROPONI: If anyone wants to convey that message to him, I'd appreciate that. Just for a moment -- I don't want to keep you. It's been a long day for many people. But

I'm troubled by this discussion of balance and see-sawing and teetering and whatever we want to call it.

It's our concern that when we talk about, we may be asking a secondary question -- we should step back a moment -- and this is a question, I think, we should ask is when we're designing a new program to combat terror, does the program in its design even work? And by work, I think the definition should be does it actually demonstrably improve our ability to combat and stop terrorism? If it does not or if we cannot conceive of a way that it can using the current technology or understanding of what the capabilities of the technology are, then that idea ought to be scrapped. It shouldn't be balanced.

It shouldn't be counter to liberty or privacy or any of the other things we hold dear. It really ought to be put in the dust bin, taken out, and thrown away. If, however, we've got a good idea, then we ought to do what you all are talking about which is finding ways, I think, to embed privacy principles within that program from the very start. I hope you will do that with good ideas.

With bad ideas, I'd throw them away. One of them that I think was designed exactly backwards and which I think we probably missed this opportunity to deal with is Secure Flight. Congress has mandated this. It seems we're going to be stuck with some sort of program to do passenger screening. Unfortunately it seems from recent reports that TSA and DHS have moved headlong forward towards completing this program before finding out whether or not, in fact, Secure Flight will actually do that demonstrable work of improving our security. Until that happens, I would ask you to slow down, stop, do the work that has to be done to make this program now efficient and hopefully embed it with the privacy and civil liberties principles with which I think you can gain more public acceptance of this program. I just want to make one other quick comment.

I am concerned, and I think the ACLU is broadly concerned that the government's efforts to combat terrorism all seem to be using this idea of the power of the technology, data aggregation, and data mining. Every newfangled system that we are coming up with seems to have as a first principle in its design architecture this idea that we will outsource a function to a private company to do much of the work that the government itself could not do under my understanding of the "Privacy Act." I'd ask you to consider that as part of your mission whether or not the government, the DHS, the TSA should be, in fact, engaged in this outsourcing of a function which I'm not sure that under the laws they can do. With that, I'll close and say thank you.

MS. O'CONNOR KELLY: Thank you very much for those wonderful comments. Are there responses from the board? Joe.

MR. ALHADEFF: Just one quick one and that was with the word demonstrably. And I think I understand that -- you know, I would fully agree that there are plenty of bad ideas whose time has not come, but they're here anyway. But the problem with the word demonstrably in an area where we really have very little idea of the effectiveness of what we're doing is almost an impossible proof point. And I think what you have to do is set around the parameters of what are reasonable, likely to succeed, potentially effective. And

then over time, you can get to the word demonstrably, but I don't know that when you're at the idea stage demonstrably can necessarily be made. I think what you do is you talk about how closely is the objective and the means are related and whether there are less obtrusive and intrusive ways to get to there. That's the first, I think, area of inquiry.

Demonstrably is the proof point once it's been in effect for a little while because then the question is when you have something running, you can try to start to figure out whether it's being effective or not. At the conceptual phase, I think there are perhaps different parameters of analysis that get you some part of the way to identifying the bad idea or quantifying the effectiveness of the idea. But I don't know that the word demonstrably, because we have so many open parameters at some points in time, can necessarily happen at the time of the concept.

MS. O'CONNOR KELLY: Other thoughts from the committee? (Whereupon, there was no response.)

MS. O'CONNOR KELLY: And I see an empty podium microphone. So I think we will thank the speakers. We have two questions on comment cards and I actually undersold the idea of the comment card because it gives you the opportunity to comment anonymously which I think is an important opportunity in any world. The first question is, is it possible for the committee to identify a personal privacy threshold? What are the factors that must be present to cross the threshold into personally identifying information or the collection of personally identifiable information? Tara.

MS. LEMMEY: The -- obviously the committee hasn't taken any of these issues up yet, so we're all speaking on our own behalf. But in the exploration work that I've been involved in so far, it's really focused on the notion of predicate which hasn't come up too much today yet, but will come up a lot in, I think, our future discussions. For any particular event, what is the predicate, what is the reason, and then how do they move forward from a mission basis on that? And as you start to explore the -- all of the various aspects of security as we heard in this morning's speakers different -- there are different predicates and different purposes. And so it's hard to say that there's one framework.

MS. O'CONNOR KELLY: Other thoughts on the committee?

MR. MARSH: One of the things of privacy, I think, that we have to keep in mind is that the definition of privacy very frequently turns on an individual's assessment or definition of privacy. There's some people who have no hesitancy to disclose their income or to disclose their health or marital status or age. Other people are terribly offended and feel that it's a trespass when people get into those areas. So I think you have to separate privacy for the individual as to how they perceive privacy from a general standard of what a citizen or what a nation affords, what areas of protection are given privacy regardless of the preferences of individuals. But I think you have to watch privacy a little bit and you need to define it because it differs from individuals to individuals.

MS. O'CONNOR KELLY: Thank you. We have one more very interesting question. Are there lessons to be learned for protecting personal privacy from the FBI's Witness

Protection Program and what process is in place to protect and/or distinguish personal privacy from virtual privacy? (Whereupon, there was no response.) (Laughter.)

MS. O'CONNOR KELLY: We have stumped the committee. We'll have to leave you hanging for the next meeting for an answer to those two questions. With that, we have, I think, completed the public comment period. And I'm going to turn the gavel over hopefully briefly to Paul for a little open discussion among the committee, perhaps not necessarily to decide anything in the few minutes we have remaining, but to at least begin the work of assigning tasks and even thinking about subcommittee assignments in the future. So, Paul.

MR. ROSENZWEIG: We've learned a lot, so I guess the agenda gives us this little bit of time plus our next meeting and time between now and the next meeting to figure out what we're going to do with it. So I'd be interested -- I'm happy to offer my own views. But rather than do that, I'll -- I'd like to step back and ask any of the committee members what their take on some of the recommendations are. Should we be thinking big or should we be thinking small, should we be thinking programmatically or should we be thinking technologically based, et cetera, et cetera, et cetera? What particular programs should we focus on if we're going to be focusing on programs? We're not going to make any decisions right now, so feel free to express your personal viewpoint. And since it's easier for me, if you raise your hand or something like that, I'll try and keep a little list. Howard.

MR. BEALES: I think it's important for us to attack something concrete. I think to attack -- the complexity of the issues here is such that it's very easy to get lost in generalities and accomplish nothing useful and provoke a lot of pointless disagreement, unless we attack something that is concrete and really joins the issues in a particular context. I think a likely candidate for that is screening programs in general, whether it's screening programs in general or a particular screening program. You know, I think quantitative risk assessment tools have proved extremely useful in a lot of places where you can -- where there's good and frequent outcome measures like credit decisions and fraud issues. Their utility in this context is less clear. Their privacy implications are just as great and I think it's a very important issue for this group to think about.

MR. ROSENZWEIG: I have Sam, Michael, and James.

MR. WRIGHT: I agree with Howard's comments, but I also recognize the fact that we are an advisory board and it seems to me that it would be -- I personally would think it to be very useful and I think would be useful to other members of the board if DHS came back to us and said here are the issues on which we are seeking your advice so that we have some sense, not that it will be determinative, but some sense of the department's priorities in this area.

MR. ROSENZWEIG: Michael.

MR. TURNER: I'd like to concur with Howard Beales. I do think at least methodologically there's more value to be added by starting with something specific and inferring general lessons from that, whether it's Secure Flight or another application of

program. I'd like to caution, though, with that approach that this committee might be stuck in the unwitting position of having to defend or amend the particular case study. Per the remarks of the gentleman from the ACLU that we have to establish demonstrable matrix of the efficacy of a particular program which invariably would come out of such a case study or would come out of the scrutiny of the committee from not addressing that in the case study. So that is just a cautionary note. I do agree with Alhadeff and I think here that we need to consider also the potential unintended consequences because if we're looking that a program works or doesn't work, what is the objective? And if we look at Secure Flight -- and I'm thinking here with an economist hat on -- the stated objective is to increase passenger security. But unstated objectives might be accomplished that might be lost if the program were scrapped. For example, if it makes a majority of Americans feel more secure to have their -- the backgrounds of their fellow passengers screened and, therefore, they feel comfortable flying, if they lose that program, it may threaten the viability of our commercial airline sector. So -- and that's something that -- it seems pie in the sky, but needs to be considered. So, you know, these are the decisions that we'll need to make as we grapple with the methodology, but it's certainly something that I would put before you.

MR. ROSENZWEIG: James.

MR. SHEEHAN: With the caveat that this is somewhat extemporaneous in that we've just been here for a few hours dealing with these rather large subjects, I was enamored with the suggestion that the big and the small join in something symbolic or paradigmatic like Secure Flight. And perhaps by attacking or looking at something like that, we might get -- be able to sink our teeth into something that's real and also grow into something larger and really attack or address the entire problem. Also with a little bit of tongue and cheek, I say that something like -- I'm reminded of the Paris peace talks, the Vietnamese War Paris peace talks. We're going to have to figure out the shape of the table on this balance, equal, maximum situation about what we do with privacy and security. We're really going to have to come up with some language that captures what it is we'd like to see happen between privacy and security in order to be able to move forward at all.

MR. BEALES: I think we ought to optimize. (Laughter.)

MR. ROSENZWEIG: Next on my list is Ramon. Then I have Joseph and Charles and Joe.

MR. BARQUIN: I'm going to go ahead and shoot my wad. I got three comments. The first one is that while we've heard from just about everyone else in the Department, heard ourselves, the general public, we really haven't heard from the Chief Privacy Officer and her office in terms of what are the pain points, what are the real issues that she has to battle in the trenches every day. And I think that would be important insofar as she is the principal agent or broker, you know, recipient of our advice, number one.

Number two, I would like to at least make sure that we consider, going back to pragmatics of my buddy, Joe Leo, here, that we consider timing. There are things that while undoubtedly they're very important, given the amount of time that we're going to be spending and the sparseness of our meetings, et cetera, it's just not terribly realistic that we're going to be able to make a contribution. As a matter of fact, it may be something

where we as individuals, you know, wearing our own other hats might tackle and make a contribution then. But insofar as a committee, I think this timing and pragmatics of the issues are very important.

And last but not least, while we have heard once or twice -- it sort of crept into the discourse of the day, but I think it's at the root of what we're about is ethics. We really haven't talked about ethics in any significant way and I think it needs to largely underpin just about everything that we're going to do later on.

MR. ROSENZWEIG: Great. Joseph.

MR. ALHADEFF: Thanks. And I just wanted to highlight. I think John may be trying to get your --

MR. ROSENZWEIG: Sorry. I keep looking around. If you don't see it, put up your little flag till I've got you.

MR. ALHADEFF: So as far as I was looking at it, I mean I think there -- we also have to pay attention to a Socratic dimension to what we're doing here. And I raise that for two points. One, because I thought everyone else had mentioned a Greek philosopher and it was kind of bad if I didn't. (Laughter.)

MR. ALHADEFF: And, two, because I think we're focusing a lot on end points and we have to think about the process too. And the process in our case is definitely going to be iterative. And I think one of the things about the process is if we don't keep notes on our process, which the open forum helps us do in a tremendously good way, we also don't understand our own analytical framework. And part of, I think, the most important thing we're going to develop is ways to think about the issues. We may or may not come out with a result that is useful or acceptable or taken on board. We may or may not come out with a result that gains consensus. But the process with which we come out with the result may be one of the most important things we do. And I want to make sure that we pay attention to the process.

MR. ROSENZWEIG: Okay. Right now I have Charles, Joe, John, Joanne, and Lisa, Tara. Anybody else? David. Okay. Remember that we stay here as long as you keep talking. (Laughter.)

MR. ROSENZWEIG: Okay? So I know that that's no incentive to end because I've been on many panels like this. Anybody else have to leave that wants to get on right now? The cue will continue to remain open. Okay. Charles.

MR. PALMER: Well, I have to say this has been a fascinating day and as the -- I'm beginning to get the feeling -- once again, I'm the token propeller head over here since I'm not a policy wonk and I think I will be very soon. A couple of -- just a couple of very small points. I like the idea of a real program. Let's look at the real thing. I think that's -- but that's indicative of my background. But the difference is we want to make sure that we have impact. We don't want to become yet another committee. To be declared a yak is just not much fun. And I'm on this for four years. (Laughter.)

MR. PALMER: So impact, I think, is important. And the idea of going after Secure Flight or this or that program, that's fine with me, but let's make sure the train is not so far out of the station that it just doesn't matter. And the other point on balance or leveraging or whatever we want to call it, again as a geek, I want to point out that a lot of the problems we've talked about today are because we can't do security right. Security and privacy, okay, you can describe it any way you want. The way I describe it is security enables privacy. Without security, don't bother. And so we are -- I mean, security is not officially in the title of our committee, but to talk about privacy without security is sort of a waste of time.

MR. ROSENZWEIG: Joe.

MR. LEO: Just real quickly, thank you, Ramon, for acknowledging my pragmatic hat. And I wanted to add to that, yes, I wanted to ask Nuala as well. But I think we have an opportunity in the short term since we have a -- the department has a brand new Secretary and a deputy security and the deputy secretary seemed quite eager -- Mr. Jackson seemed quite eager to interact with us that one suggestion may be that if we do come up with an idea or two or three to get cracking immediately on that, we ask the secretary/deputy secretary what's on their mind for immediate governance, that we may help contribute in the, you know, almost real time now. And as you acknowledged, there's a four-year journey ahead for most of you. I only have two. A four-year journey, so can we for impact make an impact now to help the leaders of the Department of Homeland Security ferret out some things that we might be able to contribute to. And that's it.

MR. ROSENZWEIG: I'd have to agree with that. That's sort of why I asked the deputy secretary to tell me what was on his mind. John.

MR. SABO: I agree and I like the idea of focusing on tangibles that are vital. But I think we have a little work to do to frame our own approach to those specific programs. I heard maybe four or five levels of discussion that we've been advised the committee should look at. One, you know, you think of what is in the "Privacy Act" and the motivation for it. However inadequate it may be in the environment of private data sharing, you've got "Fair Information" practices that are part of the law and DHS is subject to that. And one of them is security. So it isn't like security is not addressed. It's an inherent part of the "Privacy Act" and it talks about the -- and that's true for most accepted "Fair Information" practices. So I think we're covered there and it's an important piece. The real question I'm having that we need to tackle is we need to deal with larger predecessor issues.

You always make the assumption that someone has made a viable business case or public policy case for a system or an application. And, yet, we've been hearing a lot of, you know, speakers and even our own panel talking about the viability of the system, that is do they have a valuable output, a result. Will implementing a billion dollar system actually eliminate terrorists coming in to the air traffic system? So all I'm saying is we -- even if we tackle specific things, I would say that we should at least set up our parameters. Do we want to examine advisory system because of the impact on privacy? In other words, tackle that. Then do we want to tackle the whole issue of managing privacy responsibilities in that system? And then another area is risk management, you know, quantification. Are there methods to quantify this that are meaningful to DHS and to the public and finally

some form of audit or ongoing assessment? Those may not be the right categories, but it seems to me we -- if we're going to tackle an ad hoc system, we should at least come at it from a principal set of principles or approaches.

MR. ROSENZWEIG: I'm going to exercise chairman's prerogative just to follow up. So your answer to that is yes? I mean, the Secure Flight Program, for example, you know, one way to approach it would be to say Congress has made a decision -- I mean, this is akin to what David Sobel said -- Congress has made a decision. The best use of our time would be to try and make it work. Another way might be to say step back and offer our independent advice on whether or not Congress has made the right decision. I take it you're advocating the latter being part of the discussion?

MR. SABO: I think it could be if we agree that's a tier of the discussion. In other words, the thing that struck me about the OMB PIA assessment guidelines was that they didn't address about half of the requirements of the "Privacy Act." They also, as I understood it, they kind of made an assumption that the program managers put into the system are really doing the right thing. So we're hearing a lot of sensitivity around that whole issue that as soon as you begin moving into this new modern world of data sharing and private/public and technology, there are issues at play that haven't been fully addressed by anyone before. So it could be -- I am saying yes, but I'm saying we may want to have -- segment out our advice, deal with some of the mechanical things -- I don't mean to diminish them, but -- and a hard focus on those even as we look at the broader issues.

One other comment and I'll shut up, and that is NIST has done a lot of work in the last year partly in response to "Homeland Security Act" around a whole set of publications and federal information processing standards for security, the life cycle of security. And guess what? They can -- you can assess a threshold -- one of our speakers talked about it -- a threshold of security. If your sensitivity of the data and the risk and so on meet a certain level, the system is assessed at level three, and now you need to put in certain controls. There's a whole life cycle of that. There's nothing on privacy. And it could be that this threshold idea is an area of focus for us as well.

MR. ROSENZWEIG: As we move along, I'm going to make a last call. I have Joanne, Lisa, Tara, David, and Reed. Does anybody else want to be on the list? Lance. Although, Lance, you're going to be -- unless I -- and, Nuala, don't worry. You are going to get the last word. (Laughter.)

MR. ROSENZWEIG: Does anybody else want to be on this list before I put a line under it? (Whereupon, there was no response.)

MR. ROSENZWEIG: Okay. I'm putting a line under it now. Joanne.

MS. MCNABB: Let me first say my name is Joan. It looked like Joanne. And her name is Nuala. (Laughter.)

MR. ROSENZWEIG: Sorry, Joanne.

MS. MCNABB: That's all right. Okay. Pretty much what I'm going to say has been said. The one thing I'd like to especially say is I'd like us to look at a time line, sort of two lines. One is the time line -- Nuala's time line or the department's time line or what are the things that are most pressing? And then for us to look at a time line of the order in which we would like to address them both from meeting their time line schedule and actual -- and also in sort of a logical progression.

I agree that -- with many people that starting with the concrete programs, things look like a good idea, but I'm rather drawn right now to Howard's approach to slightly broadening it a bit. So take the issue of screening in general, we'd probably be looking a lot at Secure Flight if we took that issue, but there are a lot of other programs we could be looking at also, both for models and for other things that are coming up. And I think that that issue of screening raises almost all of the key issues of data integrity, which is a big part of the challenge there, of data mining, of using private sector information, the way the "Privacy Act" could or doesn't apply to that. And I think it would be a very good place to start.

MR. ROSENZWEIG: Lisa.

MS. SOTTO: Thank you. I'd just like to echo Joe's comments about this being an iterative process. I think that that's absolutely right. And for me, this has been very instructive because the more we listen and talk amongst ourselves, I think we can reach some consensus as to what issues are the most important ones to tackle. On a slightly different note, I find it interesting that we have not heard the use of the term RFID today. I think it's important that we consider some of the more intrusive technologies. It can be argued, of course, that they are only vehicles that get us to better -- theoretically better security and not part of the bigger picture that we ought to tackle. But I think that they are -- because they are considered so intrusive, we ought to think about them in whatever program we decide to pursue. Thank you.

MR. ROSENZWEIG: Tara, you're next.

MS. LEMMEY: I think that we need maybe perhaps some time to come up with a framework collectively because I don't think we're all -- and it's come up a little bit here and there -- but we're not all on the same -- we're not of a mindset yet for a process approach. So I think if we tackle the problem right now without having a framework, we'd be cats running in different directions and not really saying, okay, these are the ten things we can all agree are important.

Some of the things that -- go on that kind of list for me that keep me up at night right now are some of the issues that we heard from the governor about why and what and how. And that focuses on the predicate issue for me. And then secondary and tertiary uses because what starts to happen with policy is it's, well, there may be a privacy policy for the first use around a predicate, all of a sudden, the thing starts moving and what we've seen is the nested policy issue starts to go nonlinear pretty quickly. And will the system work, which is the question that we had come up here, which then leads you into the transparency audit oversight and redress issues.

And I think maybe just having a collective discussion on framework would be useful. And then what we've experienced so far, at least with the Markle work -- and, again, we overlap a little bit, but not a lot -- we found that it was important not to pick one problem, but to pick a few problems to try to find the commonality so that we could put forward some policy thinking that was overarching instead of being very specific to one program. So it may be worth it for us to take on -- two different -- two or three different sets of problems to just see what that bubbles up for us as we go to sort of the overarching piece. I think that's it for me.

MR. ROSENZWEIG: David.

MR. D. HOFFMAN: Yeah. I second the motion. (Laughter.)

MR. D. HOFFMAN: So a bunch of folks were quoting their favorite Greek philosophers and the folks that are doing that are much brighter than I am. So the best philosopher I can quote, who is actually the best philosopher I know, is my father, who upon the birth of my first son gleefully took the opportunity to inform me that I was now on the receiving end of the rule that trust is earned, not given, and that I will be suffering through that for the next at least 20 years of my life.

It strikes me that DHS is in the same position as a new organization and needing to earn the trust of a great number of constituencies that it affects. It also strikes me that trust is not an absolute or an abstract. Trust is something that is situational. You trust some people to do your taxes, but you may not trust them to baby-sit your children. So I think in the context of privacy oftentimes you may -- different constituencies may trust DHS with certain data to do certain things, but not other things.

So that leads me to the conclusion that it is particularly important for us to pick a specific situation, a specific case study to analyze. I do believe actually Secure Flight would be an excellent one for us to analyze because I think it will cause us to explore a lot of the broader issues on which we can give some significant guidance to the organization. Specifically I think it brings up a number of different constituencies that are affected by it, that it will be exceedingly important for us to analyze, obviously the individuals, including citizens and non-citizens whose data will be analyzed, the media, who seems to have taken great interest in the program, foreign governments, who will need to express, I believe, their view of how data should be shared that might potentially go into that. I also believe that it brings up the important issue of transparency that we've talked a lot about.

Also an issue about proportionality. Are the goals and the benefits that will be secured from the program worth some of the dedication of resources and the provision of data that it will provide? And also I think the issue of mission. What will the data be used for and how do you control that over time? So the last part of my long soliloquy is that whenever I have a new lawyer come in to work for me, I always start off with a specific direction to that new corporate lawyer which is to say that they have two roles. They play a control role and they also play a counseling role. And as part of that counseling role, I feel that it's very important that in their first meeting with the general manager of the business unit that they are going to be counseling that they ask that general manager what are the things that

you really want to do that you feel you can't do because the lawyers won't let you do it. And I feel like we didn't hear that today. I feel like we didn't hear that from your senior staff. Now, I didn't hear the things that they would really like to do that they feel that privacy is potentially impacting them. And I feel it took us down the path of really thinking of only the control part of our role, not also the counseling role.

MR. ROSENZWEIG: Reed and then Lance.

MR. FREEMAN: Thank you. Nuala said earlier that many of us stand on the shoulders of giants. I think that's right. I happen to be sitting on the left, at least physically, of a giant and that's Howard Beales. And I think that we can learn a real lesson from the Muris-Beales pragmatic approach to privacy which is to frame the issues in terms of analytically how will we choose the issues to look at and when we do, what's the framework we look at them under? It's -- Tara was speaking of that. Tim and Howard sequestered themselves, I've heard, for some period of time after they took over at the FTC, to establish that analytical framework before they did anything. And I think that is an object lesson that we -- that I urge the chair and the co- chair to insist that Howard teach us -- (Laughter.)

MR. FREEMAN: -- because the -- he is a teacher. The -- because if I'm not wrong, ancient Greece ultimately failed and was -- (Laughter.)

MR. FREEMAN: -- replaced by the pragmatism of the Romans. And so they're cute and everything, but I'd like to focus on pragmatic, analytical approaches.

MR. ROSENZWEIG: Okay. Thank you. Well, Howard, you're on the agenda for next time. (Laughter.)

MR. ROSENZWEIG: Well, no. Lance.

MR. L. HOFFMAN: Well, at the end of this long day, I have some suggested dos and don'ts, at least in my opinion. Let me start with the dos. And this gets into where we go next and to be taken up by the chair, the vice chair, the committee. I suggest we form three subcommittees process-wise. I'm going to say -- take a first cut, put something on the table as to what they might be. One would be in terms of process to get the analytical framework, things like language, that sort of thing, a subcommittee on that.

Second is on specific tasks. And here I'd say the idea of -- I'll join the bandwagon here maybe for screening programs. I like very much the idea of looking at specific -- general programs like screening programs, a specific system to look at, like Secure Flight, which would bring out all -- many of these issues would be very important, I think.

And third to address the counseling role that my -- what's the word I'm missing for somebody who has the same name? Can't remember now. Anyway, that David has.

VOICE: Homonym.

MR. L. HOFFMAN: Not homonym. VOICE: Namesake?

MR. L. HOFFMAN: Namesake. Thank you. Namesake. A research committee, how to plan for research or how to look into the future. And this is also where DHS could go if they wanted to and say we have these future things. We don't know quite what to do about it, but can you consider looking at it? Okay?

So, in essence, a committee on process, a committee on specific tasks, like screening programs, and finally a what's next, research, things like RFID, matrix, international implications, you name it, put it there. Okay? Have those three subcommittees to look at what they might want to do and would be appropriate. Okay. Those are the dos.

The one don't I would have is I'm a little leery of getting fogged down in what to fix immediately because, you know, some deadline is coming up or -- that's what the employees of DHS are supposed to be doing. So they can go and talk to us and so forth and get our counsel, but I don't think that should be a charge for the committee as a whole if we're going to have a lasting effect that will work in the long run. And the only -- the last thing I want to close with is I sure would like to get some guidance on how to pronounce Nuala. What is the -- (Laughter.)

MR. L. HOFFMAN: -- preferred pronunciation?

MR. ROSENZWEIG: It's Nuala -- no. It's Nuala. She'll tell us, I'm sure. Okay. Well, that kind of closes it. Before we turn to Nuala -- said it right, yeah, there you go the group that we believe are the best use of our resources is at a relatively practical level kind of specific to particular programs or clusters of programs like screening. Screening seems to be the leading list member right now, but I don't think we should jump to that until we've kind of plumbed the depths of whether, you know, behind that or in front of that should be things like RFID. But I hear the sense that we want to be practical.

I hear the sense that we think that at least part of our remit is the broader question of whether or not this works or whether or not this makes sense from a broad perspective even if you might think that that issue was already pretermitted by congressional determination. I think that's probably a good idea. I hear in particular, though, overarching both of those a sense from the committee members, especially from what Tara and Lance just said, that we need to do some work in the near future more concretely on defining what it is, the processes by which we're going to act, and what it is we think our outcome is. I sort of would capture that as saying, you know, what is our deliverable going to be, if anything? Is it going to be a summary of the state of the art, a concrete set of recommendations, a technical appendix from those members of the committee who feel like they have that technical expertise, which I certainly would never put myself in that category? I think that those are all issues that need to be kind of worked through in the near term hopefully so that we have a resolution of them available for -- or a proposed set of resolutions for them available for our next meeting. That would be kind of the mission statement I would take from where we are now. But that's without settling on it because we need to talk a little more. Have I -- does anybody think I've misstated or inaccurately kind of captured the feeling? Okay. Well, feelings don't mean decisions, so that's okay. I guess I'll leave it to Nuala to give us the last word amongst which I've asked her if she has any answer for Ramon.

MS. O'CONNOR KELLY: I do. Thank you for bringing up the question, what it is we need help with since that is why we created this committee in the first place. Someone close to me said, I can't believe you're putting together this committee. You're admitting that you don't know what you're doing. And I said, you know, either I'm a strong enough ego to admit when I don't know what I'm doing or I see the wisdom and the value in formalizing the conversation with the public, which is really what I see this committee as doing, and bringing the best minds to bear on the issue because these are important issues.

And we don't -- although I've tried to hire everyone I can in this community, we don't have the ability to hire all of you full time. You're too expensive, so we've gotten you for free. Thank you very much. Let us not -- let us remember just a few things.

I think Tara is right to want to set up a construct for the conversation. I would hate to see this committee get bogged down in semantics or logistics or lawyering this issue to death. I want to harken back to earlier comments that this is a real-world problem that has, I think, real-world solutions and affects real people. I think that there are challenges the department has been facing and will continue to face. And this organization can play a key role in coming up with concrete recommendations, solutions, best practices and principles that fit an array of programs.

I would caution against getting bogged down with any one title or any one particular program that may or may not exist. And I'm not casting dispersions of any one program. But given the Secretary and the Deputy Secretary's second-stage review, they are considering *de novo* all of the boxes in the organizations. I think we've also focused a lot on Secure Flight because you see it in the news a lot. There are many, many other similar programs that have had varying levels of success that were mentioned just in passing today.

The HAZMAT Program, for example, has many of the same issues. The U.S. VISIT Program actually is such a terrific bunch of privacy people. They volunteered to come and give a presentation today and I said there wasn't time on the program, but they share many of the same concerns. I got many, many moments of wise counsel. And Peter is still in the room, so I will give another nod to Peter Swire 'cause he was, I think, after my husband the second person I called the day I got this job. And he said focus on three things. You've only got time to do, if you're lucky, three things. And I'm trying to remember now actually what the first three things were. (Laughter.)

MS. O'CONNOR KELLY: But I'm so tired, I can't remember. I know one of them was setting up an office structure and a privacy structure for this department that would hopefully last well beyond my tenure at the department, which includes a great, strong privacy team at headquarters, which we certainly have, and privacy officers throughout the department.

I think the second agenda was such a pressing need for international cooperation, which we have devoted a tremendous amount of time to and hired some tremendously strong people to work on.

And I think the third issue is one that we haven't solved yet and I think that may be one for your consideration which is creating a framework for the places -- there was a concept I remember writing a paper in college on the place where the clothing gaped as a metaphor for something, blah-blah-blah. But the place where the law gapes here, the place where the "Privacy Act" fails to cover the use of private sector data, the use of data that has not contemplated a now 30 plus year old statute. And I think that brings us all the way back to the Choice Point scenario.

How does that experience affect the Department of Homeland Security and affect the trust agenda, affect the faith the United States, the people of this country have in this department? The big issues that are facing -- that keep me awake at night are not necessarily the ones I thought that were going to face us when I came into this job.

The concept of transparency in an organization that necessarily has to do some activities in a secretive manner, meaning law enforcement and counter-terrorism activities, which would be damaged if the public -- if they -- the facts of them at the time the investigation was going on saw the light of day.

How do you keep accountable and how do you hold accountable an organization that necessarily for its operation and for the safety of its employees cannot tell you at all moments what it is doing? Now, that is a big picture, public policy issue that I think may be beyond what we want to do at this committee, but it is something I throw out there because the "Freedom of Information Act," which was added on to our charter well into the first year of our office's existence, has become for me one of the most focal points of my concern about the operation of this federal government. It is both one of the strongest statutes internationally and I think also one of the most overlooked. And that's actually where I give David Sobel tremendous credit because FOIA again is an arcane and not well thought out -- I mean, not well considered often in the public space statute, but one that can be incredibly potent and incredibly powerful in holding our leadership accountable. I think the comments from the speakers were incredibly well-taken, particularly in the concept of due process.

It was somebody on my senior team who said to me just before this session if we could solve one problem for the Department of Homeland Security, it is how people can get off the list, I mean, so to speak, in the colloquial term. How do we create again accountability and due process for screening programs that are not transparent, that are not accountable, that are not allowing people to know even what it is they're being accused of when they're being deprived of a right such as a HAZMAT driver's license or the ability to get on an airplane? I completely agree with the idea that functionality has to be considered at the premise.

Oftentimes Becky, who plays an entirely different role in our office, which is running our PIA Program, which contrary to what Steve Cooper thought, we actually do in our office and it's not 33,000 programs. I don't think that's the right number. But she finds herself and the team that works with her on that frequently asking the very core questions about the *raison d'etre* for these programs. In simply asking a question why, why are you collecting this data, why is this data point necessary, we are asking developers and

program managers and program advocates to go back to the very beginning, I think oftentimes making for a better and more effective program by asking the threshold questions. So I think you can do more than one thing.

I think Paul is right to not try to bite off too many different and disparate projects and thus get lost. I counsel against getting bogged down in the semantics, although I think that the language we use to describe this problem is incredibly important. And I was very mindful of listening to our various speakers who I did not coach in any way. In fact, many often used words that I would not use such as balance in getting this issue right. The three projects, I think, actually are very similar to the ones Lance suggested. And, again, I would use Secure Flight and U.S. VISIT and TWIC and HAZMAT and Registered Traveler and the many, many screening programs this department does as case studies for a screening concept, a screening module, a subcommittee that considers what are the core elements, what are the core values we as a country demand that our federal government embody in any program that is going to ask us for personal information before allowing us to blank, fill in the blank, get on an airplane, have a driver's license, et cetera, et cetera.

What are we going to demand in terms of due process, access, redress rights? Those principles, if this committee could articulate those principles for us, I think that will have precedential effect not only for the Department of Homeland Security but for every federal agency that engages in some kind of similar activity. I think that is the -- from the most concrete to moving on to a more sublime and aspirational and forward-looking, technologist-focused subcommittee, something that encompasses RFID and biometrics and looking forward to new technologies that perhaps we haven't even considered yet. I think the question is very well-taken.

What is it you want to do? I loved David's concept of counseling. I've always thought that was the much more fun part of being a lawyer, to be a counselor, to be an advocate and a help mate of the business process. That is how I see our office at the Homeland Security Department and I think that is as it should be, but in still asking the core questions, why at the very beginning. I would say in response to that that in my conversations with the deputy secretary and the secretary, they both do want to consider the fullest range of technologies that may allow for efficient, cost-effective, and more accurate screening operations, homeland security, counter-terrorism activities, et cetera. They are not afraid to use new technologies, but nor should we be bamboozled by the potential for these new technologies to do wondrous things that somehow are unimaginable to us. As my dad says -- and, again, the great philosopher king -- you know, my dad said I don't care about all the new technologies in the world. If that guy next to me in line in the airport has smoke coming out of his sneakers, I want somebody to stop him from getting on that airplane. (Laughter.)

MS. O'CONNOR KELLY: So let's remember there is the high tech and the low tech. But I think there is an opportunity for this committee and for my office to play a championing role, a championing of the -- foregoing the chilling effect that the privacy discourse sometimes has on new technologies, new thoughts. And instead we can say let's consider it, but let's also as a concomitant to the technology development build the privacy protections in, into the very code.

So I think that an RFID, biometrics, technology working group would be certainly something worth considering. But I think lastly, the very issue of data, data collection technologies, even as a separate technology group, data mining, data usage, anonymization, the very data points of the alphanumeric data that is collected about you, combining the concept of the use of private sector data and how that may or may not be in the breach of the "Privacy Act," may be also a separate sphere encompassing the Choice Point, Bank of America, Lexus, Nexus situation, which do impinge upon the Department of Homeland Security as that data is often used or can be used in screening programs. And, again, I would say that the Department leadership is open-minded as to the potential utility of such, but also the potential harm in importing private sector data in a permanent way into the Department of Homeland Security or any other federal agency.

So how we can help our program leaders think of the best practices, the rules of the road for those separate spheres, screening as an operational concept, new technology such as biometrics and then data as its own world encompassing private sector sources and technology would be my thoughts for some of the projects you might consider.

MR. ROSENZWEIG: Great. Well, thank you. That adds more to our plate. Just remember, we're only 20 unpaid people. (Laughter.)

MR. ROSENZWEIG: I guess it's up to you, Becky, now to, as our designated federal officer, to suggest we end.

MS. RICHARDS: So I move to adjourn the DHS Data Privacy and Integrity Advisory Committee.

MR. HOFFMAN: Second.

MS. RICHARDS: Hereby adjourned.

(Whereupon, at 5:25 p.m., the above- entitled meeting was adjourned.) CERTIFICATE OF NOTARY I, GEOFFREY L. HUNT, CVR-CM, the officer before whom the foregoing testimony was taken, do hereby certify that the testimony of said parties was taken by me by stenomask means and thereafter reduced to typewriting by me or under my direction; that said testimony is a true record of the testimony given by said parties; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this testimony is taken; and, further, that I am not a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of the action. This certification is expressly withdrawn and denied upon the disassembly or photocopying of the foregoing transcript of the proceedings or any part thereof, including exhibits, unless said disassembly or photocopying is done by the undersigned court reporter and/or under the auspices of Hunt Reporting Company, and the signature and original seal is attached thereto. _____
GEOFFREY L. HUNT, CVR-CM Notary Public in and for the State of Maryland

My Commission Expires: _____